5. COMMUNICATIONS VIEW

The Communication View provides two models of the ICS: 1) a communication framework showing the protocol stack used in ICS, and 2) a description of the CEOS Network and Internet usage between Retrieval Managers.

5.1 ICS Communication Framework

This section defines the communications stack to be used for implementing CIP over the networks between ICS *Retrieval Managers*.

5.1.1 ICS Utilization of TCP/IP

ICS Compatibility: Mandatory

ICS will be implemented using the TCP/IP set of protocols [R20 and R26]. Note that CIP is required to not be limited to TCP/IP (see requirement 336 in [R2]), allowing some CIP applications to be implemented over an OSI communication stack, for example. But, ICS shall exclusively be TCP/IP. In ICS, CIP and IGP will use TCP. ICS addressing will be according to Internet domain, host name and port id, format. The use of TCP services by CIP and IGP are defined in the following sections. An identical communication configuration is adopted by GEO Servers to allow interoperability.

5.1.2 TCP/IP Services

ICS Compatibility: Explanatory

This section provides an overview of the layering of CIP and HTTP over TCP/IP. This overview supports the discussion in the next sections on specific TCP calls by CIP and HTTP.

TCP/IP has 4 conceptual layers of software. Starting at the top is the application layer, supported by the Transport layer, supported by the Internet Layer, and the Network Interface Layer. A hardware layer supports this stack. (See [R12] for a more extensive review of TCP/IP.)

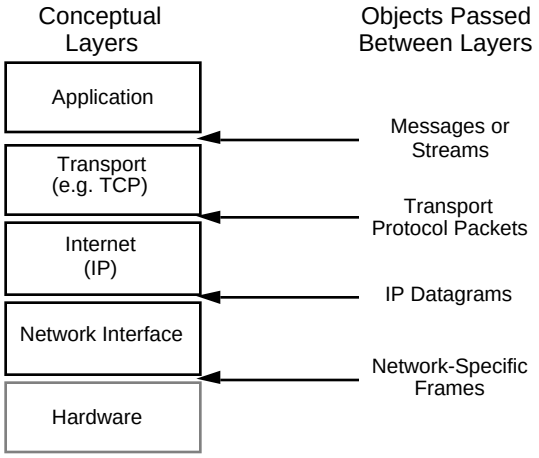

Figure 5-1. TCP/IP Internet Layering Model

The interface between the Application Layer and the Transport Layer for TCP is defined in [R26]. An Application must use the TCP Application Commands shown in Table 5-1 to send messages over the network. TCP accepts the commands listed in Table 5-1 from an application and must also return information to the application it serves. When an application wants to communicate with a remote application, TCP must establish a connection. A connection is a logical communication path identified by a pair of sockets, one at each machine. A socket is identified by an Internet address and a TCP port.

Table 5- 1. TCP Application Commands

Command	Description
Open	This command establishes a TCP connection for the application. A Passive open sets the connection to Listen for an incoming connection. An Active Open forms a connection with a specific remote socket.
Send	This command causes data to be sent on a connection.
Receive	This command allows data to be accepted from a connection.
Close	This command causes the connection specified to be closed.
Status	This command returns data to the application about the state of a connection.
Abort	This command causes all pending Sends and Receives to be aborted, the connection state is deleted, and message is sent to the TCP on the other side of the connection.

5.1.3 CIP Translators and TCP Communication Stack

ICS Compatibility: Explanatory

The implementation of the communication protocol stack for ICS is shown in Figure 5-2. CIP applications within the *Retrieval Manager* and *CIP Client* will create CIP messages which can be encoded using Z39.50. Z39.50 is an application level protocol and produces a byte stream which is passed to the Transport Layer using a TCP socket. TCP establishes a virtual circuit with the remote site and sends Transport Protocol Packets to the Internet layer. The Internet layer implemented with IP, passes IP datagrams to the Network Interface.

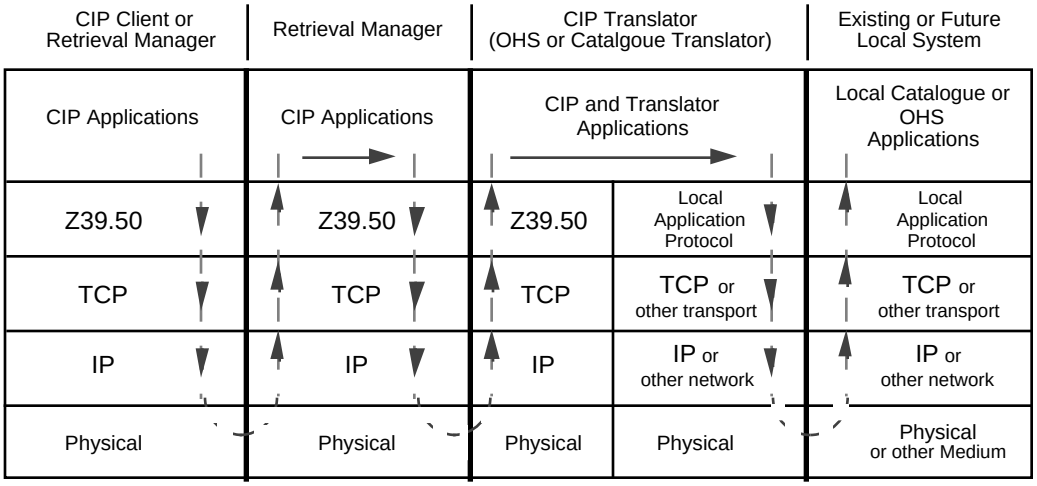

Figure 5-2. ICS Layered Communication Model

The specific example shown in Figure 5-2 shows a *CIP Client* (or a *Retrieval Manager*) establishing a *CIP Session* with a *Retrieval Manager*. Messages are passed down the protocol stack in the *CIP Client* with each layer encapsulating the message with its layer-specific information until they can be passed to the physical network to the other site. Note that there may be multiple devices in between the physical devices hosting the *Client* and the *Retrieval Manager*, e.g. routers. The messages are unpacked on the way up the protocol stack in the *Retrieval Manager*. In this particular example the message continues on from the *Retrieval Manager* to a CIP Protocol Gateway through a packing and unpacking cycle. In the application level of the CIP Protocol Gateway, the message may under go much translation to change the application semantics of the message from the CIP domain to the legacy system domain. The CIP Protocol Gateway then wraps the legacy application system message in the protocol specific to the legacy system communication stack. This allows the message to be passed from the Gateway to hosts within the local system, which in turn unwrap the message and answer the message at the application level.

5.1.3.1 Implementing CIP using TCP/IP

ICS Compatibility: Mandatory

This section defines the interface between CIP and TCP services. This section summarizes a memo by Clifford A. Lynch [R13] and extends the topics to CIP. (Lynch's memo was written for Z39.50 Version 2 and has not been updated for Version 3.) Table 5-2 provides the mapping of CIP messages to TCP Commands. When a CIP message is to be sent via TCP, the TCP commands listed in Table 5-2 are used.

Table 5-2. Mapping CIP Messages to TCP Commands

CIP Message	TCP Command
InitializeRequest	*Open* to establish a connection, then *Send* the *InitializeRequest* data using the open connection
InitializeResponse, SearchRequest, SearchResponse, PresentRequest, PresentResponse, SegmentRequest, DeleteResultSetRequest, DeleteResultSetResponse, AccessControlRequest, AccessControlResponse, ResourceControlRequest, ResourceControlResponse, TriggerResourceControlRequest, ResourceReportRequest, ResourceReportResponse, ExtendedServicesRequest, ExtendedServicesResponse	*Send* to an established connection
Close	*Send* the CIP *Close* data, then *Close* the TCP connection.

Connection. In the Internet environment, TCP Port 210 has been assigned to Z39.50 by the Internet Assigned Number Authority [R16]. To initiate a *CIP Session* with a *CIP Target* in the TCP/IP environment, a *CIP Origin opens* a TCP connection to port 210 on the *CIP Target* and then, as soon as the TCP connection is established, *sends* an *initializeRequest*. The TCP connection can be closed by either the *CIP Client* or the *Retrieval Manager* by sending a *close* message and then closing the TCP connection.

Encoding. The CIP specification and the Z39.50 standard specify application protocol data units (APDUs) in Abstract Syntax Notation One (ASN.1) [R14]. These APDUs include EXTERNAL references to other ASN.1 and non-ASN.1 objects such as those defining record transfer syntax to be used in a given application association. Standard Basic Encoding Rules (BER) [R15] are applied to the ASN.1 structures defined by the CIP profile and Z39.50 protocol to produce a byte stream that can be transmitted across a TCP/IP connection using the *Send* command.

As the approach above is based on a Z39.50 Implementor's Group agreement, the mapping of GEO messages to TCP commands is done the same as shown for the CIP messages in Table 5-2.

5.1.4 Distributed Session Management

ICS Compatibility: Mandatory

The need for Distributed Session Management when using CIP is illustrated in Figure 5-3. A user may request a search which results in sub-searches to other *Retrieval Managers*. To accomplish this, the *CIP Client* forms a *CIP Session* with a *Retrieval Manager*. In order to send the sub-query to the second *Retrieval Manager*, a second *CIP Session* between the two *Retrieval Managers* is established. In the first *Retrieval Manager*, the second *CIP Session* must be associated with the initial *CIP Session* between the *CIP Client* and the *Retrieval Manager*, so that results are returned appropriately to the client which initially requested the search. The set of *CIP Sessions* needed to achieve the users request is referred to as a *User Session.*

The GEO DOGS that is used to initiate a session with a *Retrieval Manager* maintains a connection for one user session and terminates the connection with a close. Hence, each time a GEO user requests *CIP domain* data, a new connection is established. Similarly, when a *Retrieval Manager* accesses the GEO Servers for data, a single Z39.50 (version 2) session is initiated for each user. At the end of the user session the connection is closed. All the GEO specific requests from the *CIP domain* are serviced via this interface.

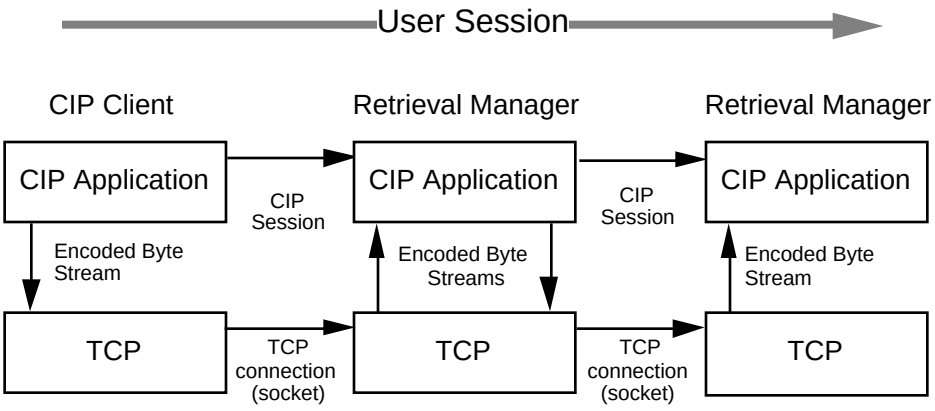

Figure 5-3. Distributed Sessions

The management of distributed sessions is accomplished in the following fashion.

- Individual *CIP Sessions* are based on Z39.50 associations. Z39.50 is a single client to single server protocol, i.e., it does not provide for distributed session management across several *Retrieval Managers*.
- CIP defines a unique, mandatory Reference ID for each message, which is used to manage message tracking.

- The *Retrieval Manager* is required to manage associations between incoming CIP messages and subsequent secondary messages to other ICS elements and to GEO Servers. This is accomplished using the session management logs defined in Section 4.

So, the management of distributed sessions is accomplished by the session logs which are established in the *Retrieval Managers*. A session log is established for a user during the initialization of a session. For each CIP request which the *Retrieval Manager* receives it maintains the association with any secondary request in the session log. When the secondary response is returned, the session log is consulted, the appropriate primary session is determined and the primary response is sent.

5.1.5 Implementing HTTP using TCP/IP

ICS Compatibility: Mandatory

IGP is implemented using the Hypertext Transfer Protocol (HTTP) Version 1.0 [R18]. HTTP is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, object-oriented protocol which can be used for many tasks, such as name servers and distributed object management systems, through extension of its request methods. A feature of HTTP is the typing and negotiation of data representation, allowing systems to be built independently of the data being transferred

HTTP communication usually takes place over TCP/IP connections. The default port is TCP 80, but other ports can be used. This does not preclude HTTP from being implemented on top of any other protocol on the Internet, or on other networks. HTTP only presumes a reliable transport; any protocol that provides such guarantees can be used. Within ICS, IGP using HTTP is implemented over TCP/IP.

The HTTP/1.0 protocol is based on a request/response paradigm. A client establishes a connection with a server and sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content. The server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity meta-information, and possible body content. A separate TCP connection is established to fetch each URL. In this approach, the use of inline images and other associated data often requires a client to make multiple requests of the same server in a short amount of time.

5.1.6 Directory Services

ICS Compatibility: Mandatory

Key to a distributed three-tier architecture (Section 2) is the use of a directory service. As mentioned in Section 2, ICS uses a simple directory service for the conversion of high-level names to network address. Additional directory services are not currently used by ICS, e.g., to resource location service, Yellow Pages services, mail address lookup. Based on these requirements and based on the choice of TCP/IP, the Domain Name Service (DNS) is used in ICS.

To perform a search, a specific collection must be targeted in the search. The syntax which CIP requires for collection names follows a URL structure. The URL contains an Internet domain name for the Retrieval Manager on which the collection can be found. DNS contains information about the mapping of host and domain names, such as, "eos.nasa.gov", to IP addresses. DNS is maintained in a distributed fashion, with each DNS server providing name service for a limited number of domains. Also, secondary name servers can be identified for each domain, so that one unreachable network will not necessarily cut off name service.

An additional directory service is needed when a Retrieval Manager chooses to implement the Public Key Infrastructure for authentication. ICS uses the Lightweight Directory Access Protocol (LDAP) for interacting with a Certification Authority. LDAP is a TCP/IP version of the X.500 Directory Service which is defined by the ITU-T (formerly CCITT) [R23]. The ITU X.509 Directory - Authentication Framework defines authentication services are provided by the Directory to its users. The Directory can usefully be involved in meeting their needs for authentication and other security services because it is a natural place from which communicating parties can obtain authentication information of each other: knowledge which is the basis of authentication. The Directory is a natural place because it holds other information which is required for communication and obtained prior to communication taking place.

5.2 CEOS Network Connectivity

This section defines the connectivity between ICS *Retrieval Managers* provided by the CEOS Network. This section contains the following information:

- An overall CEOS Network Architecture
- Bandwidth for Browse Image Data

5.2.1 CEOS Network Architecture

ICS Compatibility: Explanatory

The CEOS Network Subgroup is developing a network for CEOS usage, called CEOSnet. An overview of how ICS uses CEOSnet is presented in this section. See [R8] for detailed information about the CEOSnet. The CEOS Network Subgroup maintains a WWW page at http://nic.nasa.gov/ceos-ns/index.html.

The CEOSnet architecture is shown in Figure 5-4. Within each participating agency or country, a *Retrieval Manager* is provided. It is the intent that the users in a country use that country's national Internet (or other national network resources) to access its local *Retrieval Manager*. To satisfy user requests, a *Retrieval Manager* may then need to access data from another participating *Retrieval Manager*. Two network alternatives are available to provide this access. One alternative is to use the worldwide Internet. While the worldwide Internet is quite ubiquitous, its performance is not dependably high.

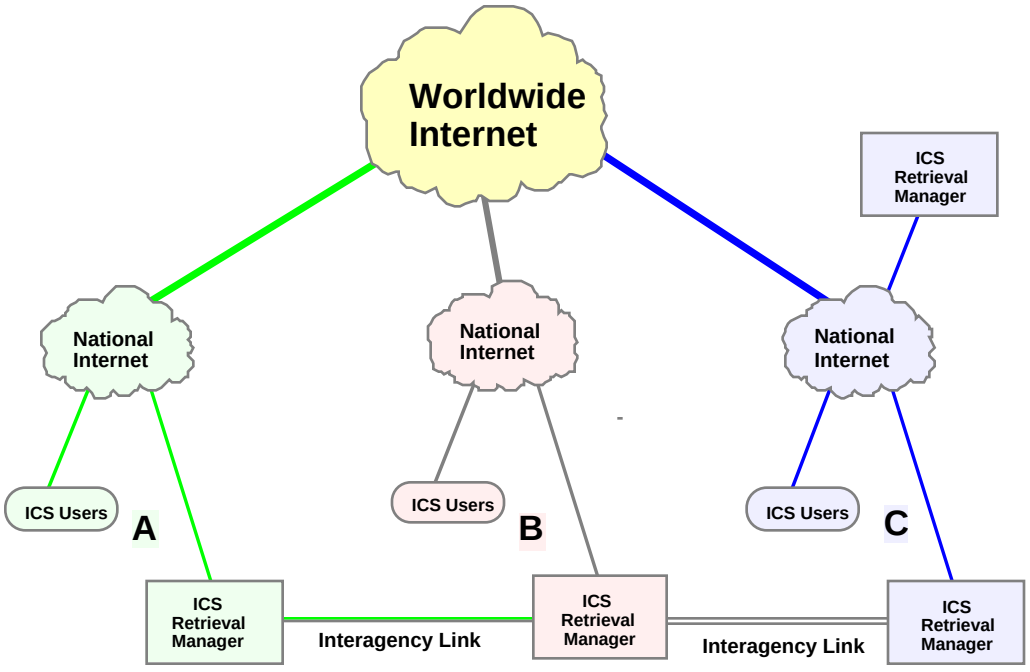

Figure 5-4. ICS Networks Model

On an individual, bi-lateral basis, the participating CEOS members may choose to implement private circuits between their facilities. These private circuits can be made available for access to *Retrieval Managers*, and may or may not also provide connectivity for other bilateral services. Collectively, these private circuits between participating CEOS organizations constitute the CEOS Network (CEOSnet).

CEOSnet is a limited access network coordinated and maintained by CEOS agencies, affiliates, and observers to support CEOS tasks and activities by providing access to and sharing of global Earth observation data and information. Access on or through the CEOSnet resources is only authorized when that access is in conjunction with CEOS approved activities and programs, the funding agencies for the CEOS Network links approve or agree to the use, and capacity on the CEOSnet links is adequate to support the use. Additional uses of CEOSnet will be allowed as approved by the CEOS agencies, affiliates and observers providing the CEOS Network resources. CEOSnet is not to be used for commercial gain or profit. (See [R27] for details on CEOSnet acceptable use policy.)

Note that the CEOSnet is thus not a separate network consisting of a distinct set of circuits and equipment, but instead is a logical network of components provided by participants and used for CEOS purposes.

The nominal data flows to satisfy a user query is:

1) User accesses local *Retrieval Manager* via national (or agency) network resources
2) *Retrieval Manager* contacts cooperating *Retrieval Managers* via CEOS net (preferred) and/or the worldwide Internet as appropriate.
3) Cooperating *Retrieval Managers* access local database resources to formulate response.
4) Responses are returned to originating *Retrieval Manager* via same network which carried the request.
5) Originating *Retrieval Manager* collects the responses, and delivers them to the user via the national or agency infrastructure.

Note that it is not essential for an organization to have dedicated circuits to have a participating *Retrieval Manager*. Subject to performance limitations, the worldwide Internet provides the connectivity required. In Figure 5-4, dedicated links are shown (as an example only) between agencies A and B, and between B and C. In this example there is no dedicated link between A and C.

Note that technically in Figure 5-4, it is possible for the *Retrieval Manager* at A to access C via the pair of dedicated links (A-B and B-C). However, policy issues must be resolved by each agency for this to be allowed. Otherwise, the worldwide Internet can provide connectivity between A and C.

The *ICS Client* has network options for accessing CIP items on remote *Retrieval Managers.* For example, assume that a user connected by a national Internet to *Retrieval Manager* B in Figure 5-4, performs a distributed collection search which matches a collection on *Retrieval Manager* C. If the user wishes to perform a product search on the *Retrieval Manager* C collection, the *ICS Client* could send the search either to *Retrieval Manager* B which would forward the request or the client could send the request directly to *Retrieval Manager* C. (Information in the collection identifier supports the search request in either path.) By sending the search to *Retrieval Manager* B, the interagency link between B and C is used which will probably outperform the path from B to C as it involves the Worldwide Internet. In general, *ICS Clients* will want to make use of the Interagency Links between *Retrieval Managers.*

The TCP/IP protocols will be used for communications between ICS *Retrieval Managers*. Interconnected routers in the CEOS Network must support network protocols which are robust and consistent with existent Internet protocols and standards (see [R20] for applicable standards). All interconnecting networks attaching to CEOS Network are at least IP-based relays to other networks or user sites. Additional network protocols or enhancement features are allowed but should not affect the network availability, performance, or interconnectivity.

5.2.2 Bandwidth Considerations

ICS Compatibility: Explanatory

A driver in the amount of CEOS Network bandwidth required to support ICS users is the retrieval of browse images. The CEOS Browse Task Team has begun to develop several parameters needed to support an estimate of the CEOS Network bandwidth necessary to support ICS user's request for browse images. Estimates for the browse image data are based upon the statistics from the existing guide data and the anticipated user behavior.

First, a bandwidth estimate for the browse data is presented. The first parameter in the Browse bandwidth estimation is the browse data size after compressed (to transfer via WAN). A maximum size is 1MB for EOS-HDF browse size with other agencies browse size is less than about 200 KB. So, an average browse size is estimated to be 500 KB.

The next parameter to be estimated is the user's expected time for transfer of a browse image. Current performance for DLR and the University of Rhode Island provides image retrieval from 45 to 60 seconds per browse data. The Browse Task Team suggests that a desirable requirement is 30 seconds.

The next parameter for estimating the bandwidth for a given ICS node is the frequency of browse retrieval requests. Given that CIP is a session oriented protocol, one approach to estimating the number of browse requests is to estimate the number of concurrent sessions. The number of sessions will have a diurnal variation, but only the peak number of sessions and the related peak

number of requests are important for estimating the needed bandwidth. Also as the purpose of the worldwide ICS is realized, the diurnal variation of requests at a *Retrieval Manager* will be reduced as more users are retrieving data from around the globe. The ICS URD requires the *Retrieval Manager* be designed to be capable of supporting a peak load of a minimum of 100 concurrent user interaction sessions. It is expected that all ICS data providers should support a minimum of 30 simultaneous sessions for a *Retrieval Manager*, this includes remote sessions to remote *Retrieval Managers*. The CEOS Browse Task Team estimates an average of 10 sessions. This number is 1/3 minimum multiple sessions requirement for ICS URD as some sessions of CIP are used for catalogue retrieving and ordering.

If we assume that this 1/3 fraction of users is continually executing browse requests these numbers provide the following network bandwidth requirement:

500 KB * 10 sessions / 30 sec = 1333 Kbps

We use a similar method of bandwidth estimation for the guide data. The existing browse data has an average size of 40 KB. Using this basis and the method above we can see that the network bandwidth requirements for the guide data would compute to:

40 KB * 10 sessions / 30 sec = 106 Kbps

The combined bandwidth for the browse image and guide data will be:

106 Kbps + 1333 Kbps = 1440 Kbps ~ 1.5 Mbps (T1)

Of course, this estimate will change as the parameters are estimated by each agency. So, this bandwidth requirement is only a guideline.

This page intentionally left blank.

6. SECURITY VIEW

This section provides the security architecture for ICS. This section contains three parts. First, an assessment of the need for security in ICS is presented. This motivates the second part which presents the system design for a secure ICS.

6.1 ICS Security Assessment

The purpose of the ICS Security Assessment is to explain the need for appropriate security risk mitigation measures addressed in Section 6.2.

6.1.1 ICS Security Needs Overview

ICS Compatability: Explanatory

ICS is an international catalogue interoperablity program accessible to users on a global basis. Built on an open-computing network architecture to facilitate access by a wide variety of users, the driving requirements of its security architecture are integrity, availability, and confidentiality of its data assets. The project vision is open access to well-pedigreed data in which users may have confidence, while maintaining certain proprietary and administrative data in confidence.

Integrity. Because of the scientific nature of the project, integrity of project information is critical. The accuracy of the collection, product, guide and browse data must be stored and accessed in a fashion which maintains the integrity of the data. In addition, information to support ordering of ICS products and services must be protected against unauthorized access.

Users expect the system to guard against tampering with the source materials of the *Retrieval Managers* not only during storage, but during maintenance and distribution. Integrity threats are manifested through unauthorized access or use, leading to change, alteration or modification of information resources. The security architecture must provide adequate safeguards against these threats.

Availability. The ability to have assured use of project resources is vital to instill confidence in its users. Availability needs translate into two categories: fault tolerant features to preclude failure or operational disruption; and recovery actions, to enable timely resumption of operational activities and minimize the length of the disruption. Availability threats are manifested through denial of service events, either physical in nature (e.g., fire or loss of power) or logical (e.g., computer virus or other intrusive software).

Confidentiality. Confidentiality requirements exist because some of the information within ICS requires special protection. This includes specific user product requests and account information, and information of a private nature on individual users on the system. Information of this nature, if compromised, could result in damage or harm to ICS or to individuals. Confidentiality threats are manifested through access by unauthorized persons and authorized persons who have exceeded their privileges, e.g., unauthorized interrogation of user profile data.

6.1.2 Vulnerabilities

ICS Compatability: Explanatory

A vulnerability is a weakness in security procedures or controls that could be exploited by a threat. Vulnerabilities are often analyzed in terms of missing safeguards. Vulnerabilities contribute to risk because they may "allow" a threat to harm the system. Section 6-2, links the ICS security controls that counter the threats which may potentially exploit ICS vulnerabilities. There are seven categories of vulnerabilities which may impact ICS.

Software Vulnerabilities. Software vulnerabilities include: inadequate configuration management that permits program errors; unauthorized automated routines; and inadequacies in system and application software that may result in processing or calculation errors, or may allow unauthorized access to hardware, data, or programs. Given the collaborative nature of the software development of CEOS *Retrieval Managers*, these vulnerabilities may occur due to unintentional miscommunication.

Hardware Vulnerabilities. Hardware weaknesses include: improper operation of hardware; lack of proper hardware maintenance; inadequate physical security; and inadequate protection against natural disaster. Because all ICS hardware will be procured, installed and maintained by procedures outside of ICS, it is assumed that hardware security measures will be followed at each site. The availability of the *Retrieval Manager* at each site is contingent on this assumption. The ICS security design will need to protect against breaches of confidentially and integrity to other sites independent of hardware failures at a given site.

Data Vulnerabilities. Data vulnerabilities include inadequate access control that permits unauthorized access or authorized personnel to exceed privileges with the potential result of both accidental and malicious deletion, corruption, modification, or destruction of data, as well as theft. Of special concern to ICS are susceptibilities that impact the integrity of collections data, browse and guide data held by the *Retrieval Manager*, system configuration data, registration data, authentication data, and ordering data.

Administrative Vulnerabilities. Administrative vulnerabilities are associated with weaknesses in the effective administrative control of IT resources. They include inadequate or nonexistent administrative and security policies, guidelines, training, and controls; operating procedures (i.e., standard operating practices and procedures); management constraints, and accountability. As the administration of ICS is distributed throughout its agency members, it will be assumed that the availability of each site's *Retrieval Manager* will be dependent on the site's administrative practices. Some administrative practices will be defined by the PTT, e.g. Collection Manual [R5], but their application is dependent solely on the site's personnel. ICS must protect from losses of integrity or confidentiality from a lapse in a single site's administration.

Communications Vulnerabilities. Vulnerabilities associated with communications include: inadequate access control that allows unauthorized access to networks and communications circuits that could result in transmission interception and unauthorized access to network components; and inadequate measures to prevent circuit failure from both natural disaster and human activities, intentional and accidental, resulting in denial of service. ICS is dependent upon the CEOS Network as defined by the CEOS Network Sub-group. Individual site communication security is dependent upon routers for their sites.

Personnel Vulnerabilities. As used here, the term personnel means people who have an authorized association with ICS resources or facilities, such as: employees, certain guests and maintenance personnel, and authorized system users. This group of people is often referred to as "insiders". Insiders represent the greatest weakness in any system, including ICS, because they already have access, usually understand the system configuration and operation, and may be aware of existing vulnerabilities. Security weaknesses associated with insiders include inadequate physical and logical controls that allow an insider access to systems beyond which she or he has privileges; and inadequate administrative procedures or controls to minimize or detect accidents involving IT resources or IT resource theft, abuse, misuse, damage or destruction. Perhaps the greatest weakness involving insiders is that they are exposed to external influences and pressures that may provoke malicious acts against IT resources, such as destruction or theft.

Facility Vulnerabilities. Facility weaknesses include: inadequate physical security that permits accessibility by unauthorized persons which could lead to facility, and content, misuse, damage, or destruction, or theft of its contents; and inadequate protection against natural disaster that may result in the damage or destruction of the facility or its contents. Furthermore, poor facility maintenance and services, such as poor housekeeping, poor air quality, temperature extremes, and power fluctuations may result in damage to or destruction of IT resources.

As the ICS resources are distributed throughout its agency members, it will be assumed that the availability of each site's *Retrieval Manager* will be dependent on the site's facility practices. ICS must protect from losses of integrity or confidentiality from a lapse in a single site's facility.

6.1.3 ThreatsÄ

ICS Compatability: Explanatory

ICS is concerned with threats that exploit the above vulnerabilities and have a detrimental impact on the integrity, availability, and confidentiality of its IT resources. Generally, threats to ICS resources come from two major sources: natural disaster and human activity.

- Natural disaster includes: airborne particles, cataclysm (earthquake, volcanic eruption, tidal wave, etc.) , fire, static electricity, and weather. Note that these threats will exploit vulnerabilities at specific sites affecting availability over which the ICS system design has no authority. But ICS must preclude lapses in confidentiality and integrity to other sites given a natural disaster, i.e. contain any threat to the single site.

- Human activity includes activity from both authorized persons and unauthorized persons.
  - Authorized persons are users, employees, and maintenance personnel who have some level of authorization to use or have access to ICS resources. Threats resulting from authorized activity may be accidental (an incident without malice) and intentional (a malicious act). This may include otherwise authorized persons who exceed their authority. This may also include errors or omissions in the software development or the intentional or accidental inclusion of malicious code, e.g. viruses.
  - Unauthorized persons are users or persons who do not have authorization to use or have access to ICS resources. Even though in theory, activity by unauthorized persons can be accidental, this section treats all such activity as intentional.

6.1.4 ICS Security Definitions

ICS Compatability: Explanatory

The following definitions are used in the ICS with respect to security concepts.

Authentication: Verification of the identity of a user or, validation of a communication (the second part provides for non-user based authentication, e.g. between *Retrieval Managers*).

Authorization: Permission, granted by a properly appointed person or persons, to perform some action.

Confidentiality: The protection of information from disclosure to those not intended to receive it.

Data Integrity: The assurance that data received is the same as data generated.

Domain: A system or portion of a system which has the same security policies and requirements. Individual agencies determine the boundaries of domains.

Non-repudiation: The ability of the receiver to prove that the sender of some data or of a request did in fact send the data even though the sender might later desire to deny ever having sent that data.

Proxy: A software agent that acts on behalf of a user.

Registration: The process whereby an individual submits required personal information to an agency and, in return, the agency provides the means (e.g. login name and password) necessary to perform authentication with the agency's system.

6.2 ICS Secure System Design

6.2.1 Overview of Secure System Design

ICS Compatability: Explanatory

The ICS security controls are divided into three groups: administrative, physical and computing.

- Administrative security controls are policies, guidelines, and practices and procedures designed to manage and implement security.
- Physical security controls are physical barriers or devices designed to prevent harm to or loss of IT resources and assets, such as access control card readers, intrusion detection systems, and fire suppression systems.
- Computing security controls (sometimes called technical security controls) are software mechanisms designed to prevent harm to or loss of data and information.

Table 6-1 maps the vulnerability categories, discussed above, against the security control categories. The remaining sections in this chapter describe the specific security controls in each control category of administrative, physical and computing.

Table 6-1. ICS Vulnerabilities versus Security Controls

Vulnerabilities	Security Control Category		
	Administrative	**Physical**	**Computing**
Software Vulnerabilities.	CEOS ICS Software CM ICS Event handling Security Testing	Site facility protections *	Standards on RM development Fault Handling
Hardware Vulnerabilities.	Site hardware administration *	Site facility protections *	RM Response to Unavailability of Remote RM
Data Vulnerabilities.	ISA back up procedures Authentication Information Management	Physical security of hardware *	Access control - users Access control - ISA RM DBMS data integrity functions Time Out Features Tamper Proofing Encryption
Administrative Vulnerabilities.	Collection Manual ICS Administration Manual ISA Training ICS Event handling System Rules for Users CEOS Authorization		RM Administration Independence Display System Rules for Users RM Activity Logs
Communication Vulnerabilities.		Site disaster prevention Physical security of hardware *	Network security
Personnel Vulnerabilities.	ISA Training Site personnel practices *		RM Administration Independence
Facility Vulnerabilities.		Site physical security * Site maintenance *	

* Site security controls are assumed to be in place for the sites where *Retrieval Managers* will be installed.

6.2.2 Administrative Security Controls

ICS Compatability: MAA

Administrative security controls include security policy, and other items and activities that are designed to manage and implement security policy. They should provide security guidance to users and ISAs who have some level of authorization to use or have access to ICS resources. This section defines the security controls which are listed in the Administrative Security Column of Table 6-1.

CEOS ICS Software CM. To support the establishment of *Retrieval Managers*, ICS software will be made available for reuse. This will be accomplished using a configuration controlled access point for the distribution of ICS software. Configuration Management (CM), from a

security point of view, provides assurance that the software which is available is the correct version (configuration). Configuration management can be used to help ensure that changes take place in an identifiable and controlled environment and that they do not unintentionally harm any of the system's properties, including security. Changes to the software can have security implications because they may introduce or remove vulnerabilities. The ICS CM software distribution site, e.g., an ftp site, must not allow unauthorized modification of ICS code. Once an organization pulls code from an ICS reuse library, the ICS CM is longer in effect. It is possible for an organization to cause unintended erroneous action in ICS reuse code by modification outside of ICS. This will not threaten ICS due to the domain independence of the ICS elements, e.g., access to one *Retrieval Manager* does not automatically provide access to all *Retrieval Managers*.

ICS Event handling Because the ICS operations depends on the loosely associated ISAs, procedures for dealing with events in the ICS are defined in advance. ICS events include: adding a new *Retrieval Manager*, alerting ICS to detection of an intrusion at a *Retrieval Manager*, alert of a *Retrieval Manager* being off-line either due to a planned or unplanned cause. The main communication amongst ISAs will be via an ISA e-mail list. Although for security alerts, communications must be by a separate channel than e-mail, e.g., phone, as an e-mail alert may be intercepted. The procedures for ICS event handling will be detailed in the ICS Administration Manual.

Security Testing Security testing is conducted to ensure that the security features meet technical specifications and to locate vulnerabilities. Examples of security testing tools are: Security Administrator Tool for Analyzing Networks (SATAN) and Internet Scanner, a product of Internet Security Systems, Inc. (ISS). These tools are designed to discover weaknesses or holes in a UNIX based network and recommend fixes. Procedures for ICS security testing will be detailed in the ICS Administration Manual.

ISA Training In order to insure consistent ICS operations and adherence to procedures with security implications, ICS Training will be conducted for ISAs. This training will cover, at a minimum, the material in the ICS Administration Manual.

System Rules for Users ICS users cannot be expected to act responsibly with respect to ICS operations, unless they are aware of the system rules for users. These rules should clearly delineate responsibilities of and expectations for all individuals with access to the system. Often rules should reflect logical security controls in the system. For example, rules regarding authentication should be consistent with technical features in the system.

Management Authorization The authorization of a system to process information, granted by a management official, provides an important quality control. By authorizing processing in a system, a manager accepts the risk associated with it. Management authorization should be based on an assessment of management, operational, and technical controls. Since the SDD establishes the security controls, it should form the basis for management authorization, supplemented by more specific studies as needed. In addition, periodic review of controls should also contribute to future authorizations. Re-authorization should occur prior to a significant change in processing, but at least every three years. It is important to identify the appropriate management authorization for ICS. ICS is a CEOS activity and has the context defined by its interfaces (see ICS Context Diagram in Section 3). For ICS, the authorization must come from both the appropriate CEOS organization as well as individually by the agencies which host *Retrieval Managers*. The ICS is planned and authorized by the Access Sub-Group. Each agency operating a *Retrieval Manager* is represented in the Access Sub-Group.

6.2.3 Physical Security Control

ICS Compatability: Explanatory

Physical security controls are designed to guard against threats that result from both natural disaster (e.g., storms and resulting power outages) and human activity (e.g., fire, theft of hardware and software, physical access to a facility by unauthorized persons). All physical security controls listed in Table 6-1 are the responsibility of the sites which host a *Retrieval Manager* and therefore are not under the control of the ICS SDD.

ICS as a system is robust to a failure of physical security control at a single site, i.e., a security failure due to physical controls may cause a loss at the site but cannot result in a loss at another ICS site. Each *Retrieval Manager* is independent from a security authentication perspective such that the integrity of data is not threaten by a lapse in physical security at another site. From availability consideration, the loss of a particular *Retrieval Manager* could cause disruptions in the operations of ICS. The event handling measures described in Section 6.2.1 and the System Management in Section 7, provide for the response procedures which would be initiated in case of a *Retrieval Manager* failure due to a lapse in physical security control.

6.2.4 Computing Security Controls

A summary of Computing Security Controls is provided in the first part of this section. The remainder of the section describes the authentication in ICS and the Group Security Model.

6.2.4.1 Summary of Computing Security Controls

ICS Compatability: MAA

Computing security controls are software and firmware mechanisms used to limit access, detect intrusion, detect malicious logic and prevent its propagation, etc. This section defines the computing controls which are listed in the Computing Security Column of Table 6-1.

The following Computing Security Controls are required to be implemented in the *Retrieval Manager* based on requirements in the ICS URD [R2], Sections 3.1.2 and 3.2:

- Standards on *Retrieval Manager* software development
- *Retrieval Manager* Fault Handling
- Access Control (See also SDD, Section 6.2.4.2)
- *Retrieval Manager* DBMS data integrity functions
- Session Time Out control
- RM Administration Independence

The following Computing Security Controls are required to meet the ICS security design. Requirements will need to be added to the ICS URD [R2] to insure the ICS elements are compatible:

- Retrieval Manager Response to Unavailability of a Remote Retrieval Manager
- Display System Rules for Users

It is important to note that Network Security is covered as a CEOS Network Sub-Group topic. Network security covers the issues outside of the application level *Retrieval Manager* Security functions, e.g., IP address blocking in a communication router.

6.2.4.2 Authentication Mechanism

ICS Compatability: MAA

This section describes several topics which introduce the ICS design for authentication. First the two mechanisms provided by CIP are described, then two scenarios are described for a *target* authenticating an *origin.* This section address the application layer provision for authentication which CIP provides. It is also important to note that *Retrieval Managers* make use of IP address as a basic authentication of other *Retrieval Managers.* . In addition, the IP address of the clients can also be used for user authentication and validation. This concept is discussed later in this section.

To meet the ICS security requirements in the ICS URD [R2], a comprehensive approach to network security based on a well developed cryptographic mechanism is needed. Authentication occurs in the context of a *CIP Session.* A *CIP session* is composed of multiple CIP *operations.* A CIP *operation* consists of several messages. A CIP session is begun with an *initializeRequest* and ends with a *close*. The authentication protocol described below allows authenticated sessions as well as authentication for any specific operation.

Three mechanisms are provided in CIP for authentication: unencrypted symmetric key, secure symmetric key, and asymmetric key. IP address authentication can be used to augment and simplify the authentication mechanism. In the symmetric cases, both the *target* and the *origin* are holding the same key, e.g., a username/password. In the asymmetric case, the *origin* and *target* are holding different but related keys, e.g., the *origin* holds a private key and the *target* holds a public key. Both the secure symmetric key approach and the asymmetric key approach use a digital signature as the means to authenticate the *origin.* The digital signature contains information which could have only been constructed with the user's key. The IP address authentication is not based on any type of key based mechanism and is used only for clients that have a fixed address. This mechanism can simplify the authentication by using the encapsulated information of the TCP/IP wrapper to automatically authenticate the users.

The unencrypted symmetric key approach uses a username and password in the clear, that is, there is no confidentiality of the password as it is sent from the *Client* to the *Retrieval Manager*. This mechanism is the appropriate choice when minimizing the complexity of the *Client* is a driving requirement and the risk associated with unprotected transmission of the password is minimal. Note that this approach cannot be used between *ICS Retrieval Managers.*

In ICS, the secure symmetric key mechanism is the default approach for authentication. If a *Retrieval Manager* provides authentication, the secure symmetric approach must be provided at a minimum. To provide for an agency's specific needs, a *Retrieval Manager* may choose to provide asymmetric key or unencrypted symmetric key authentication. This approach is driven by the need to comply with laws regarding export of encryption algorithms, i.e. some countries restrict the public key approach for strong authentication.

The basic element of the symmetric key approach is a Message Authentication Code (MAC). A MAC is a key-dependent, one-way hash function. A secret, shared key (password) is required to form the hash and the hash cannot be decoded. Only someone with the identical key can verify the hash by performing the same hash operation and verifying that the result is identical. MACs are useful to provide authentication without privacy. The protocol does not use privacy

as a basis, i.e., encryption is not used. The MAC for CIP is calculated using an MD5 hash. The MAC approach relies on a shared key between the *origin* and *target*. In this protocol the secret, shared key is a username/password which is particular to the user. How the *target* got the username/password is addressed in Section 7.

The asymmetric key approach is based on a set of related key pairs (public, private) used for the encryption and decryption of messages. A "digital signature" is obtained by encrypting a message hash combined with a timestamp with a private key. Such a message can be authenticated by a decryption based on the corresponding public key. In the CIP context, a client holds the private key and a Retrieval Manager holds (or has access to via a Certification Authority) the corresponding public key.

The IP address authentication is based on the nature of the Internet protocol. In most instances, the client that connects to the *Retrieval Manager* will have a fixed IP address and pass the address to the Retrieval Manager as part of their TCP/IP connection (the approach does not work for the clients systems that dynamically assign IP addresses). Once authenticated by a password mechanism, the IP address can be stored in the system area associated with the user. Thereafter, the IP address itself is used to automatically authenticate the user and set the user privileges without requesting the user for the password and going through a login procedure. This approach does assume that the user workstation is secure and only the authorized user uses the system to connect to the Retrieval Managers. If that is not the case, this approach is not recommended.

Use of CIP for authentication is shown below in two scenarios. The first scenario shows use of part of the protocol for authentication for a specific operation. The second scenario shows how an authenticated session is established during initialization of the session.

- **Authentication for an Operation**

This section addresses how a user would be challenged for authentication credentials based on a request for a CIP service, e.g., placing an order. It is assumed that the user's session is not an authenticated session.

The messages for this authentication are shown in Figure 6-1. Specific contents of the messages are provided in the CIP Specification [R3].

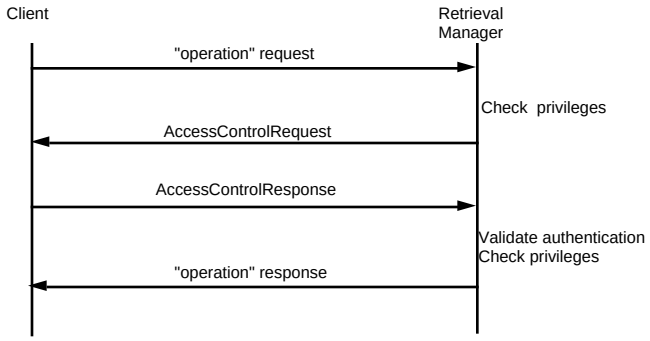

Figure 6-1. Authentication for an Operation

If Non-Repudiation is requested by the *Retrieval Manager*, another pair of messages would be needed in between *presentCredentials* and "operation" response. The first message would be from the *Retrieval Manager* to request a non-repudiated order from the client. The Client would reply with a non-repudiatable order message.

- **Authentication for a Session**

This section addresses how a user would begin a session with the intent to have an authenticated session. The authentication is a two step process. First there is a two step authentication followed by a negotiation of cryptographic options including use of a session key.

The messages for this authentication are shown in Figure 6-2. Specific contents of the messages are provided in the CIP Specification [R3].

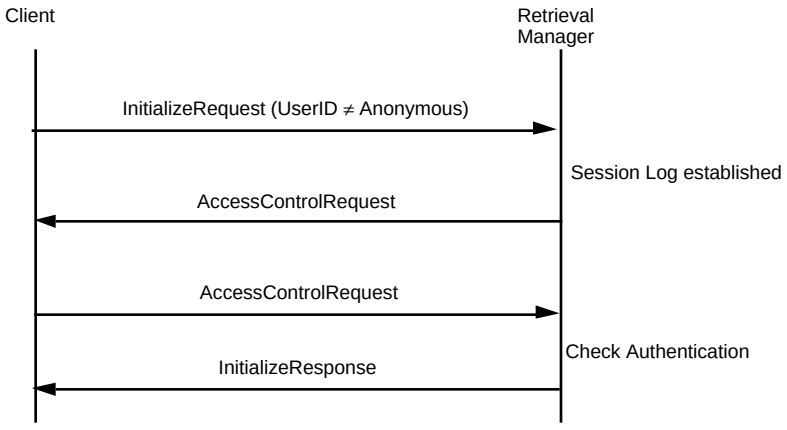

Figure 6-2. Authentication for a SessionÄ

6.2.4.3 Group Security Model

ICS Compatability: MAA

When security is considered in ICS - a distributed information system - the proliferation of credentials must be considered. The ICS has been designed to prevent a world-wide proliferation of usernames/passwords. The approach is to have the *Retrieval Managers* act as brokers for the users which they support. This avoids the user needing to be known at each *Retrieval Manager*. The *Retrieval Managers* serve as brokers based on two relationships: 1) a *Retrieval Manager* will support many users and 2) a *Retrieval Manager* is known to other *Retrieval Managers*.

The group security approach applies to any distributed session. The approach is most important when applied to ordering as ordering will require the highest security considerations. Figure 6-3 shows the focusing of orders by a home *Retrieval Manager*. "Home" in this case means that the user is registered at the *Retrieval Manager*, and for this example the user belongs to a group that has privileges to allow the order. Figure 6-3 shows multiple users sending order messages to the home *Retrieval Manager*. The home *Retrieval Manager* in turn, creates a secondary order message to the remote *Retrieval Manager* which holds the data. Each primary order from a user results in a secondary order between *Retrieval Managers*. The secondary orders are allowed based on the authentication between *Retrieval Managers* and the group membership of the local *Retrieval Manager*. The home *Retrieval Manager* maintains a cross reference of the primary order with the secondary order which was submitted to the remote *Retrieval Manager*.

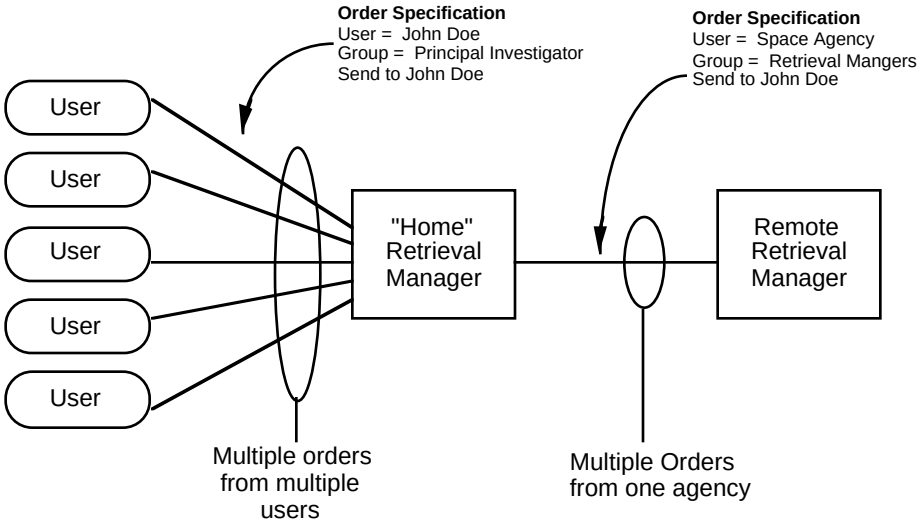

Figure 6-3. Group Ordering Model

The ordering described in Figure 6-3 and the associated text is the Order by Proxy approach. That is the *Retrieval Manager* is acting as the user's proxy to order the data on the users behalf. In the Order by Proxy case there is an agreement between agencies whereby one agency guarantees payment to another agency.

ICS also allows a second case labeled the Passthrough case. In the Passthrough Case there is a mechanism in the CIP to allow pass-through of information needed by an agency to perform its own authentication and authorization. There may be cases where agreements outlined in the Order by Proxy Case cannot be reached between agencies. Passthrough is a different method for ordering data that will provide convenience to the user. If a user who has a session established with the local *Retrieval Manager* (in Figure 6-3) wishes to order data from the Remote *Retrieval Manager* and is registered with a remote *Retrieval Manager*, the CIP can pass information (e.g. username/password) in a secure manner through the local *Retrieval Manager* to the remote *Retrieval Manager*. The remote *Retrieval Manager* then performs authentication and authorization for the user.

A scenario demonstrating the use of the Group Ordering design is shown in the next section.

6.2.4.4 Secure Indirect Ordering

ICS Compatability: MAA

This section demonstrates use of the CIP authentication mechanism to perform secure indirect ordering. Critical to secure Indirect Ordering is determining if the order should be a proxy or passthrough order. Indirect Ordering was introduced in Section 3.4.2 without discussing the security necessary if the ordered items require privileges based on authentication.

Indirect ordering involves an order submitted to a Local *Retrieval Manager* which must be forwarded to a Remote *Retrieval Manager* as the OHS which will process the order is accessible from the Remote *Retrieval Manager*. The CIP messages between the ICS elements for this scenario are shown in Figure 6-4.

Several assumptions are made concerning this scenario:

- The items specified in the order specification require privileges based on authentication, e.g., access to the data is restricted or access has a cost.
- The privileges of a user who is registered at the Remote *Retrieval Manager* will be better than those granted to the Local *Retrieval Manager* using a proxy order account, so passthrough is preferred if it is possible.
- Prior to the first step in the scenario, the User did a distributed search which necessitated initialization of a session between the Client and the Local *Retrieval Manager* and a session between the Local *Retrieval Manager* and the Remote *Retrieval Manager*. These initializations were done without authentication.

- The Local *Retrieval Manager* will support proxy ordering for this user at the Remote *Retrieval Manager* site. The scenario indicates where the Local *Retrieval Manager* can reject a proxy order if this assumption is not true.

The scenario demonstrates how the ICS RMs use CIP messages to determine if the order should be a passthrough or proxy order based on the privileges and successful authentications of the user and the Local *Retrieval Manager*. The *Retrieval Manager*s must interact on distributed information in order to resolve the decision about passthrough versus proxy. If all of the information was accessible to a single ICS element, that element could make the decision on order type based on Table 6-2. A design goal is to have the selection of proxy vs. passthrough as invisible to the User as possible. Table 6-2 assumes the Local *Retrieval Manager* can be authenticated by the Remote *Retrieval Manager*, otherwise secure indirect order is not possible.

Table 6-2. Passthrough vs. Proxy Order Decision Table

Authenticated User has privileges on Remote *Retrieval Manager***?**	**Authenticated Local** *Retrieval Manager* **has privileges on Remote** *Retrieval Manager***?**	**Authenticated User has privileges on Local** *Retrieval Manager***?**	**Type of Order**
Yes	Yes or No	Yes or No	Passthrough
No	Yes	Yes	Proxy
No	No	Yes or No	order not allowed
No	Yes or No	No	order not allowed

The steps of the scenario in Figure 6-4 are as follows:

1. A User sends an *ExtendedServicesRequest* for CIP ordering to the Local *Retrieval Manager* where the action is orderQuoteAndValidate. The order is of a direct type as it is only between the Client and the Local *Retrieval Manager* at this point.
2. The Local *Retrieval Manager* inspects the order specification and determines that the products are provided by an OHS associated with a Remote *Retrieval Manager*. The Local *Retrieval Manager* checks if the user name in the order specification is defined at the local site and, if so, prompts the user to provide a user name defined at the remote *Retrieval Manager*. The Local *Retrieval Manager* creates an *ExtendedServicesRequest* for a Passthrough order operation. Passthrough is used because, if valid, passthrough will allow the highest privileges. The passthrough order contains the user names for the Local *Retrieval Manager* and the User.
3. When the Remote *Retrieval Manager* receives the *ExtendedServicesRequest* it identifies that this is a passthrough order and not a direct order. The Remote *Retrieval Manager* checks if User is known to Remote *Retrieval Manager* UPS. If the User is known, the order will remain as a passthrough order. If the User is not known, the Remote *Retrieval Manager* checks if the Local *Retrieval Manager* is known to the Remote *Retrieval Manager* UPS. If the Local *Retrieval Manager* is know, the order will be changed to a proxy order. If neither

the User nor the Local *Retrieval Manager* are known, the order will be treated as a guest order or rejected with an access control request, asking that the User supply a user name that is defined at the Remote *Retrieval Manager* UPS.

4. The Remote *Retrieval Manager* submits the orderQuoteAndValidate *ExtendedServicesRequest* to the OHS Translator, with the possibly modified user information.
5. The OHS Translator interacts with the OHS to develop a quote for the order based on the user information provided in the order.
6. The OHS Translator sends an *ExtendedServicesResponse* to the Remote *Retrieval Manager* including the quote for the order.
7. The Remote *Retrieval Manager* sends an *ExtendedServicesResponse* to the Local *Retrieval Manager* including the quote for the order.
8. As part of the process of updating its task package database, the Local *Retrieval Manager* checks to see if the order was converted to a proxy order by the Remote *Retrieval Manager*. If the Local *Retrieval Manager* accepts serving as proxy for this User's order to the Remote *Retrieval Manager*, the Local *Retrieval Manager* will update the local task package and pass the order to the user. (If the Local *Retrieval Manager* decides that it will not allow a proxy order in this instance, the Local *Retrieval Manager* may either resubmit the order to the Remote *Retrieval Manager* as a guest order or the Local *Retrieval Manager* may reject the order and return an access control request, asking that the User supply a user name that is defined at the Remote *Retrieval Manager* UPS.)
9. The Local *Retrieval Manager* sends an *ExtendedServicesResponse* to the Client including the quote for the order.
10. The user now decides to submit the order that was quoted in the preceding steps. The Client sends an *ExtendedServicesRequest* for CIP ordering to the Local *Retrieval Manager*, where the action is orderSubmit.
11. The Local *Retrieval Manager* submits the *ExtendedServicesRequest* to the Remote *Retrieval Manager* where the action is orderSubmit
12. Because the order requires privileges, the Remote *Retrieval Manager* requires that the user be authenticated, so the Remote *Retrieval Manager* sends an *AccessControlRequest* to the Local *Retrieval Manager* requesting that the Local *Retrieval Manager* present its credentials
13. If the order is passthrough, the Local *Retrieval Manager* responds with an *AccessControlResponse* containing a MAC based on the Local *Retrieval Manager*'s user name and password. (If the order was proxy, the Local *Retrieval Manager* would first authenticate the User, using data in the Local *Retrieval Manager* UPS, before returning the *AccessControlResponse* to the Remote *Retrieval Manager*)

14. The Remote *Retrieval Manager* constructs a MAC using the user name and password for the Local *Retrieval Manager* stored in the Remote *Retrieval Manager* UPS to authenticate the Local *Retrieval Manager*. (If the authentication fails, neither proxy nor passthrough ordering is allowed. With a successful authentication of the Local *Retrieval Manager*, a proxy order would be submitted directly, i.e., jump to step 19)
15. For a passthrough order, the Remote *Retrieval Manager* sends an *AccessControlRequest* to the Local *Retrieval Manager* requesting authentication of the User.
16. The Local *Retrieval Manager* sends the *AccessControlRequest* to the Client requesting that the client present its credentials
17. The Client sends an *AccessControlResponse* to the Local *Retrieval Manager* containing a MAC constructed with the User's password.
18. The Local *Retrieval Manager* sends an *AccessControlResponse* to the Remote *Retrieval Manager* containing the MAC constructed by the Client with the User's password. The Remote *Retrieval Manager* authenticates the user by comparing the received MAC with a MAC constructed with the User's password held in the Remote *Retrieval Manager* UPS.
19. The Remote *Retrieval Manager* has now performed the authentications necessary to submit the privileged order. The Remote *Retrieval Manager* sends an *ExtendedServicesRequest* to the OHS Translator.
20. The OHS Translator interacts with the OHS to submit the order.
21. The OHS Translator sends an *ExtendedServicesResponse* to the Remote *Retrieval Manager* including the status of the order, e.g., "order being processed."
22. The Remote *Retrieval Manager* updates the order task package in the Remote *Retrieval Manager* ESDB and sends an *ExtendedServicesResponse* to the Local *Retrieval Manager*.
23. The Local *Retrieval Manager* updates the order task package in the Local *Retrieval Manager* ESDB and sends an *ExtendedServicesResponse* to the Client.
24. The Client displays the status to the User. The User smiles.

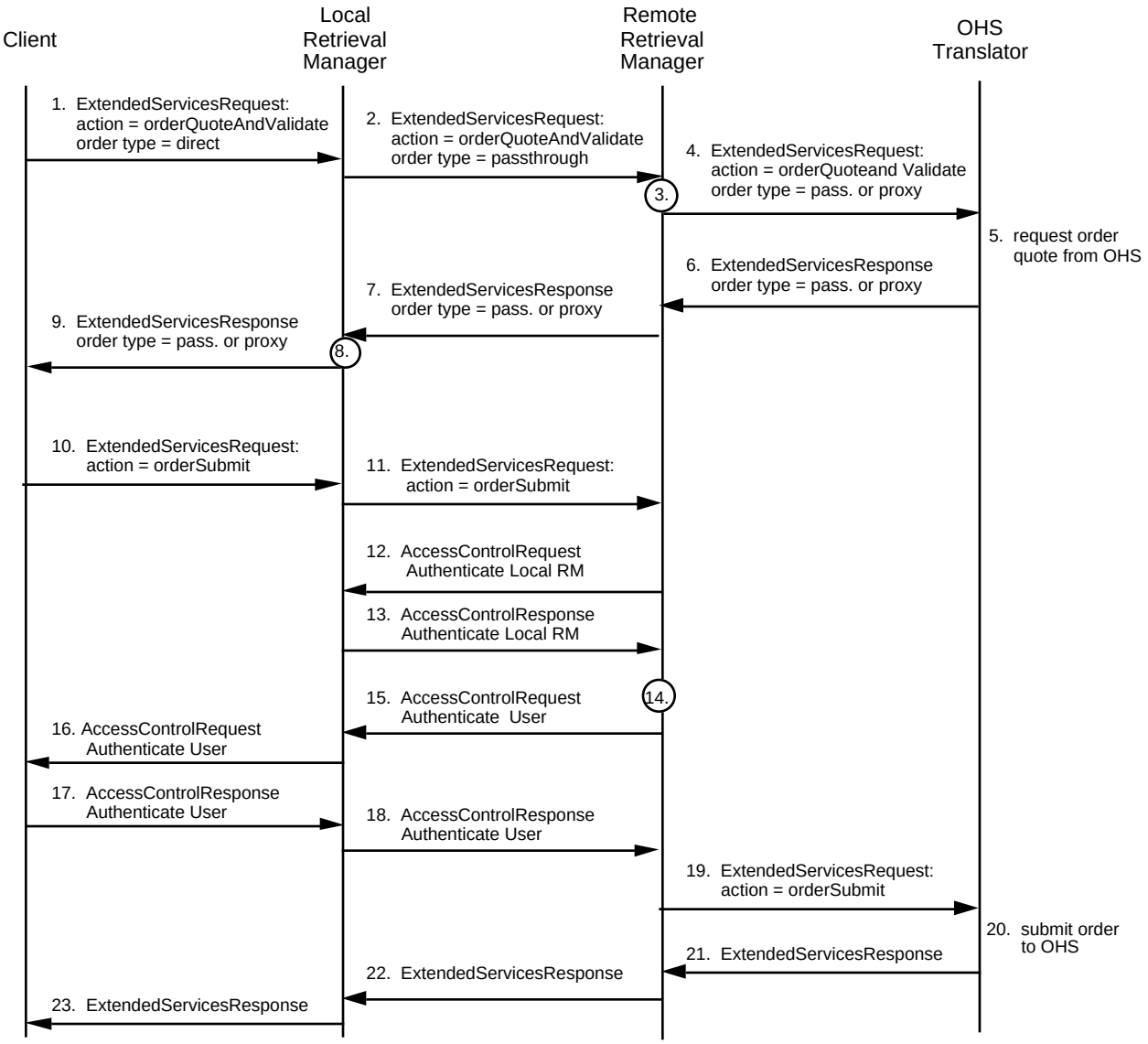

Figure 6-4. Secure Indirect Ordering

7. SYSTEMS MANAGEMENT VIEW (ICS)

The ICS Federation is a concept which describes a collection of ICS Sites. To preserve the integrity of the ICS Federation and provide some amount of assurance that each known ICS Site is compliant with the CIP and IGP Protocols, System Management functions have been identified and further described throughout the remaining subsections of Section 7. Individually these functions ensure a degree of interoperability among ICS Components; Collectively, they provide an overall picture of the compliance of the ICS System.

7.1 System Management Functions

ICS Compatibility: Explanatory

To ensure the stability and reliability of the ICS across sites while insuring site autonomy, a federation management approach to systems management has been selected. This federation management will

- Verify and Validate ICS systems that request to be included in the ICS Federation,
- Provide Daily Maintenance and Operation of the ICS Federation,
- Manage the evolution of the ICS Federation, and lastly,
- Assure Science Consistency of data held in the ICS Federation.

Collectively these four high level functions will provide the necessary structure to ensure that the tenets of the CIP and IGP Protocol and the Earth Observation Data are supported throughout the ICS Federation. Each are explored in more detail in the following sections.

7.2 Verification and Validation of ICS Systems

Before a new site can be added to the federation its compliance with the CIP and IGP has to be verified against the CIP and IGP Specifications. For this purpose an acceptance test will be performed which will evaluate the proposed ICS System against a set of ICS Functions. As a result of this acceptance test the ICS System will be marked as non-operational or as operational.

Each of the ICS Components; *Retrieval Manager, OHS Translator, and Catalog Translator*; will be tested through a series of functional tests which may span multiple components. The test scripts will be organized such that any component point of failure will be captured and recorded.

This acceptance testing that is performed will not replace the internal site testing that should be performed by the organization owning the ICS System. The acceptance testing will only begin when the agency requesting that the new system become a ICS Compliant System, certifies that the new system has passed all internal site testing.

The ICS Federation Tests results will be made available to the CEOS agency that requested the ICS verification and validation and to the ICS Federation Group responsible for Maintenance and Operations, and System Management.

The following sections provide an overview of the required testing. A detailed description of the acceptance tests will be provided in a separate document.

7.2.1 ICS Component Compliance Acceptance Test

ICS Compatibility: Mandatory

The acceptance test of an ICS Component will be based on a standardized set of test cases where every test case defines criteria which has to be instantiated for every particular test. The test cases are grouped with respect to the ICS Functions. i.e., Catalog, Browse etc.

Table 7-1 identifies each of the ICS Functions and related components that must be tested.

Table 7-1. Acceptance Testing Functions

ICS Function	ICS Components
LocalCollection Search	RM
RemoteCollectionSearch	RM
LocalCatalogSearch	RM, Catalog Translator
RemoteCatalogSearch	RM, Catalog Translator
DistributedCollectionSearch (5 or more RM's)	RM
DistributedCatalogSearch	RM, Catalog Translator
Evaluate results for Collection: Geographic Selection Temporal Selection Combinations of attributes	RM
Local Attribute Search	RM
Browse	RM
PassthroughOrder	RM,OrderTranslator
ProxyOrder	RM,OrderTranslator
Restricted Order	RM,OrderTranslator
Guest Access	RM
Status Messages for Errors	RM
Free Text Guide Search	RM,ICSGuideServer
Fielded Keyword Guide Search	RM,ICSGuideIndexer

Every new ICS Component is tested with all test cases which refer to a supported ICS Function. There are at least three possible test results for each test that is performed:

- The ICS System passes all tests. In this case the ICS System will be marked as operational for all specified services.

- The ICS System passes some tests for some components. The ICS Federation Testers will make the determination on the severity of the failed tests and decide whether to mark the protocol operational or developmental.

- Some tests fail for every function. In this case the system will be marked as non-operational.

The set of test cases may be extended to include other tests if other problems occur during the operation of the system.

The ICS Federation Testers will inform the organization that owns the system of the results of the test and schedule any future re-tests that may be necessary.
Experience with the current CINTEX federation has shown that several iterations of acceptance tests are sometimes necessary.

7.2.2 Overall Evaluation of ICS System Compliance

ICS Compatibility: Mandatory

The results of each of the above tests will be consolidated into an overall verification and validation report which will specify the details of each of the tests and the results. Further this report will specify the recommendations from the ICS Federation.

7.3 Maintenance & Operations (M&O)

Maintenance & Operations of an ICS Site will require extensive use of a Report Generation Service which will provide access to ICS Federation wide information. Types of reports that would be useful within ICS are as follows:

1)≠ Performance/Compliance - Reports to describe short and long term trends in system operation in relation to established performance criteria.
2)≠ Workload - Reports that provide statistics on the number of ICS invocations, or problem reports generated.
3)≠ Accountability - Reports which provide audit and trace capability of significant events associated with users.
4)≠ User Access Statistics - Reports which provide information for user modeling such as statistics on the types of searches users perform, number of users per month, number of product orders per user, the source and location of the orders, etc.

7.3.1 System Monitoring and Control (SM&C)

ICS Compatibility: Mandatory

The System Monitoring and control task performs the monitoring of all operational components (CIP Client, Retrieval Manager, Translators, etc.) within the ICS Federation. In addition, this task monitors the configuration of the components with respect to their location and the content. The SM&C task will establish procedures for dealing with unusual events such as component failure, new component addition, etc. in the ICS federation along with gathering statistics relating to the reliability/availability of the ICS agency member resources.

The SM&C function will monitor components on a regular interval by sending standard requests and receiving responses to these requests or by using customized scripts which invoke operating system commands to determine the status of a the ICS member agency components. The interval for conducting this activity will have been established by M&O.

The SM&C task will attempt to locate the problem if a component does not respond and inform the operator of the component of the problem. If the component will not return to operation for an extended time period, then the ICS Federation M&O will remove it from the configuration files of all gateways to make it invisible for the users until the problem has been corrected. The SM&C task will also monitor the gateways by accessing them or using automated tools to determine the status at an interval that is configurable by the M&O.

7.3.2 Valids Management

ICS Compatibility: Mandatory

The Valids Management task will provide a science and consistency check on system wide valids being defined on inventories accessible through the ICS federation. A consistency check is made to ensure that the appropriate and complete set of data requested is properly retrieved. The valids management task will review agency's proposed valids on the new inventory being introduced to the ICS federation and then approve the proposed valids or provide feedback to improve the science and consistency of the valids. The details of the process for valids management is captured in the ICS Valids Document [R4]

The Valids Management task may coordinate the local attributes being developed at various sites.

7.3.3 Federation Help DeskÄ

ICS Compatibility: Mandatory

The federation level help desk function will perform the coordination of the various ICS Agency help desks. The federation level help desk will also document and maintain a recommended list of services to be provided by each agency's individual help desk organization. The federation help desk will also provide support to agencies establishing an agency help desk for the first time.

The individual agency help desks will provide support to users of the distributed catalog system. The federation help desk will provide input to the ICS group on how to get agency help desk contact information to the users and how the user queries can be routed to the responsible agency's help desk. If the responsible agency has no individual help desk, the federation help desk will decide how to provide coverage for these situations. The federation help desk will serve as the help desk for the agency help desks. Individual user questions should not reach the federation help desk directly. It should always be brought up by an agency help desk. One agency's help desk can be designated as the federation level help desk .

7.3.4 System Wide Interoperability Interface Management

ICS Compatibility: Mandatory

The System Wide Interoperability Interface management task will provide technical consulting to agencies on details of how to link their systems into the ICS, and for any software development or customization of components needed to link into the system wide interoperability interface layer. This task will manage the set of documentation to define the system wide interoperability layer.

Within System Wide Interoperability Interface Management , the component distribution function provides the capability for technical ICS system administrative staff (M&O) to distribute new or upgrades to ICS software, database schemas, documentation and related items. A centralized approach is the most efficient method for ensuring that each ICS site receives any and all updates to ICS components.

7.4 System Management (SM)

The System Management roles and responsibilities will focus on the evolution of the system. This includes the planning for the inclusion of new system or protocol components, the modification of existing components and removal of old components. It also includes the

inclusion of new data and the update for the schemas to describe the data and the server. The SM arranges for any verification of new components. The SM also identifies all the required activities to ensure that system modifications are adopted in an orderly manner.

7.4.1 Decision Making Process

ICS Compatibility: Mandatory

The System Management is also responsible for collecting information on testing, system monitoring, and control and providing this information to the ICS federation. The system management role also includes

a) forwarding recommendations to the ICS federation
b) removal of components from the ICS federation operational baseline
c) addition of new components into the ICS federation operational baseline
d) coordinate meetings and teleconferences for ICS federation

The types of decisions and inputs that the ICS federation must provide are :

a) inclusion of new ICS site into the federation
b) recommended data access policies
c) schedule for system evolutionary components
d) removal of a ICS site from the federation
e) provide inputs to the agendas for teleconferences and meetings

8. ARCHITECTURE VERIFICATION

This chapter provides the results of several types of analysis which demonstrate that the system design described in the previous chapters will meet the ICS requirements and that the various architectural views are consistent. The analysis results in this chapter also provide design information for the developers of the particular elements of the ICS.

8.1 Query Performance Estimates

ICS Compatibility: Mandatory

Key to user satisfaction with ICS is the response times for searches. Based on the design presented in the previous sections and a set of design constraints listed in this section, estimates for the four types of CIP searches were made. Estimates for the query response times under nominal conditions are provided in Table 8-1. For detail on how the estimates were developed, see [R19]. The collection search estimates are comparable to WWW index searches, e.g., Infoseek and Alta Vista. The product search estimates are dominated by the *Existing Catalogue* search times, which are outside of ICS.

Table 8-1. Query Performance Estimates

	Collection Search	Product Search
Local Search	2 sec.	125 sec.
Distributed Search	13 sec.	136 sec.

To attain the query performance listed in Table 8-1, the design in the previous sections must be implemented as well as the following design constraints.

- Within a given *Retrieval Manager* the collection database has been well laid out and is fairly efficient with regard to the expected queries.
- The network time, including time to form Z–associations, is small compared to the time required to service a query for the network connection between a *Retrieval Manager*, the *Catalogue Translator* and the local catalogue system all at the same site.
- *Retrieval Managers* will send in parallel. For example, if a query being performed at RM_A requires subqueries to be performed by RM_B and RM_C, RM_A will send the subqueries to RM_B and RM_C simultaneously rather than sequentially. RM_B and RM_C will perform their subqueries in parallel and present their response to RM_A.
- All elements (*Retrieval Managers*, networks, translators, etc.) can be modeled as M/M/1 queues. If this is not the case, as would be the case if some element had multiple servers, then certain equations in the distributed query cases may have to be revisited. (See [R21] for a discussion of Queuing Theory.)
- *Retrieval Managers* are efficient in detecting and ignoring collection-to-collection overlap. A Retrieval Manager will not search a collection more than once during a given local collection search (regardless of whether the original query was local or distributed)
- *Retrieval Managers* will keep a CIP session open with their associated *Catalogue Translators*, such that a typical product search will not require an initialization delay between the *Retrieval Manager and Catalogue Translator*.

Table 8-2 defines the parameters used in estimating query performance within ICS. As the performance is dependent upon these parameters, the parameter values must be met to provide the query performance in Table 8-1.

Table 8-2. Performance Parameters and ICS Elements

Parameter	Affected ICS Element	Units	Nominal	Range	Source
Average collection query service time	*Retrieval Manager*	seconds	1		Logica
Retrieval Manager utilization	*Retrieval Manager*	n/a	0.5	0-0.99	Raytheon/2
Average response time required to search a local collection	*Retrieval Manager*	seconds	5		URD
Average time required to form a subquery from a query	*Retrieval Manager*	seconds	0.01		Logica
Average time required to establish a Z–association	*Retrieval Manager*	seconds	5	0-60	Logica & Raytheon/1
Average time to pass a message or response to the network	*Retrieval Manager*	seconds	0.01		Logica
Average catalogue translation service time	*Catalogue Translator*	seconds	1		Raytheon/1
Catalogue translator utilization	*Catalogue Translator*	n/a	0.5	0-0.99	Raytheon/2
Average number of collections per collection	*ISA*: collection structure	n/a	5	5-50	Delphi
Collection depth	*ISA*: collection structure	n/a	4	2-7	Delphi
Probability of overlapping collections	*ISA*: collection structure	n/a	0.7	0-0.95	Logica
Ratio of remote links to total number of links	*ISA*: collection structure	n/a	0.5	0-0.95	Logica
Average number of unique translators at a Retrieval Manager	*ISA*	n/a	1		Raytheon/2
Number of ICS sites (Number of Retrieval Managers)	*ICS System Management Group*	n/a	13	10-200	CINTEX Sites
Average response time of network transmission	*CEOSnet*	seconds	0.16		Germain
Average catalogue query service time	*Existing Catalogue* (Not part of ICS)	seconds	60	12-240	Delphi
Inventory catalogue system utilization	*Existing Catalogue* (Not part of ICS)	n/a	0.5	0-0.99	Raytheon/2

Legend for “Source” in Table 8-1:

Delphi	PTT Delphic study.
Germain	Estimate by CEOS Network Performance Test (Andy Germain)
Raytheon/1	Estimate based on translator prototype.
Raytheon/2	Estimate supplied by Raytheon Systems Corporation.
Logica	Estimate supplied by Logica.
URD	Requirement 374 in ICS URD [R2].

8.2 Scenarios

This section provides several scenarios showing the dynamic aspects of the ICS including how the scenarios are accomplished via interfaces between ICS elements and services of the ICS elements. Scenarios for both the user's and operator's activities are provided.

Scenarios in this section are organized into the following categories:

- User Scenarios
  - WWW Access to a *Retrieval Manager*
  - Existing Agency Client Access into ICS
  - Indirect Ordering Scenario
  - Guide Search - WWW Search Engine
  - Guide Search - ICS Client
  - Guide Retrieval
- Collection Population Scenarios
  - Making a CIP Compatible Catalogue Available
  - Collection Established for an Event
- System Management Scenarios

8.2.1 User Scenarios

8.2.1.1 WWW Access to a Retrieval Manager

ICS Compatibility: Explanatory

General

The scope of this scenario is to follow a user's confrontation with the system and to simulate whether a user can successfully retrieve helpful documents and EO-data from the ICS and related Catalogues.

This scenario is based on the CEO Enabling Services Scenario 1: Search for EO-data, documents and adverts [R17]

Assumptions

- The user is familiar with WWW browsers, has access to a web browser, is connected to the Internet and knows the HTTP address of a CIP/WWW Gateway.
- He has only a basic knowledge of remote sensing.
- The user works for a consultancy company that is specialized in identifying and evaluating potential water reservoirs in third world countries.

- The present project aims to build a water reservoir in Egypt. He has an explicit question he needs to be answered: Is a high resolution elevation model of this area available?
- He is interested in any documents related to this subject.
- The user has never entered the ICS before and is therefore not registered. The scenario does not include an authorization operation and the user is considered a member of the "guest" group.

Expected Outputs

The user wants to find out if a DEM of the target region is available. For the DEM data he hopes to find explicit meta-data that describes the data (i.e. browse) before he orders it. (He tries finding documents covering this subject.)

Step Sequence

1. The user enters the CIP/WWW Gateway home page for a *Retrieval Manager*.
2. He reads the short introduction about what the local *Retrieval Manager* can do for him.
3.≠ He enters the "EO-data search" interface. The user has the choice between a local or remote collection search , a data search against the entire ICS holdings (using the global node) , a local search against the entire local site holdings (using the root node), or against popular topics (using the key access nodes).
4.≠ The user chooses the local collection search of the root collection after reading the short definition supplied by the system. The form that is supplied contains fields in which the search attributes have to be entered.
5. The user selects DEM from the listed "product attributes".
6. He selects "display full valid definition" to make sure the acronym is he expected.
7. The system displays the full definition of a digital elevation model.
8. The definition is what the user expected and the user submits the local collection search.
9. After a syntax check of the search the system accepts the search.
10.≠ The system returns a structured list of collections which point to data that incorporates DEMs. One of the listed collections is called: "Elevation Models of Africa; ESA; 1992".
11. The user chooses: continue with "EO- product search".
12. The system displays a form which contains attribute fields.
13.≠ The user chooses the: "Elevation Model of Africa; ESA; 1992" and another elevation model terminal collections from the collection list. (The collection may be chosen in the collection search).
14. The user chooses the "select geographical region" option.
15.≠ This gives him the following choices:
    - type global coordinates
    - draw area of interest by polygon
    - draw area of interest by point and radius
16. The user chooses "type global coordinate".
17. He enters the coordinates for Egypt.
18. He submits the EO-product search.
19.≠ The system indicates that the search is valid after a successful syntax check has been performed.
20.≠ (Note this step was deleted from the CEO scenario as CEOS policy is to not charge for searching.)

21. The user asks for a "status monitor" to display the status of the search.
22.≠ A status monitor is displayed showing the two parallel searches (compare to step 13). The search "Elevation Models of Africa, ESA, 1992" is finished but the second search has not received any reply by the provider site yet.
23. The user selects "display product list".
24. The results of the EO product searches are displayed in a list.
25.≠ The information displayed contains information on the location, provider, title and the availability of on-line meta-data and browse data.
26. The user selects a product.
27. The user chooses the "transfer metadata" option.
28. The metadata is transferred and displayed.
29. The user chooses the "transfer browse product" option.
30. The browse product is transferred and displayed.
31. The user selects the "order product" option and orders the product delivered via ftp.
32.≠ An FTP-session is started and the product is transferred to the machine of the user. *Steps 32 and 33 are outside the ICS, but they are mentioned here for completeness purposes*.
33. The user saves this file on his hard disk.
34. The user chooses the "save EO-data search" option.
35.≠ The system saves the "data search " (the system stores this internally while this session continues).
36.≠ The user chooses the "save EO-data search results" option. (The result set is converted to a hot collection, held on the users client.)
37. The system saves the "EO-data search results".

8.2.1.2 Existing Agency Client Access into ICS

ICS Compatibility: Explanatory

General

This scenario follows both the user steps and the system software steps for an agency's user to access and order products held in the ICS collections using his local client software and an ICS gateway. The scenario concentrates on the user visible processes and the interaction between the *ICS Gateway* and the ICS *Retrieval Managers*.

Assumptions

1. ≠ User is an experienced, registered User of his local Agency (Agency A) catalogue system and is using his local Client.
2. Agency A has 2 way interoperability with ICS that is transparent to the users of its systems.
3. The User has established a session with his local catalogue systems as a registered user
4. The user is interested in AVHRR data over Europe (resident in ESA ICS holdings)
5. The user has no ICS experience and is not a registered user
6. ≠ The local agency catalogue system has been configured to recognize ICS collections through a catalog/Gateway configuration
7. Agency A and ESA have a trust agreement for authentication.
8. ≠ ESA and Agency A have a bilateral agreement that allows Agency A to act as a proxy for its users to order data. ESA bills Agency A for data ordered by its users.
9. The scenario assumes the ICS Functional Framework shown in Figure 3-3.

Agency A architecture is similar to third site in Figure 3-9 i.e., Retrieval Manager as a catalogue gateway.

Expected Outputs

The user uses his local client (*Existing Agency Client)* and finds new data through the *Retrieval Manager* which is held at a site to which his site previously did not have access.

Scenario Sequence

Search Sub-Secnario

1. Human user initiates local catalogue system client and logs in as a registered user
2. ≠ The user develops a query to discover any products containing AVHRR data over Rome taken in the 1995-1997 time frame.
3. ≠ Based on the contents of the query and information from the local agency catalogue the query is sent to the ICS Gateway
4. ≠ *ICS Gateway* translates the query from the local query language (e.g., ESQL) to the CIP Query format (RPN) and translates local agency attribute names attributes into appropriate CIP attributes
5. ≠ *ICS Gateway* interacts with the local catalogue system to determine which ICS sites can satisfy the query
6. ≠ The *ICS Gateway* acts as a ICS *CIP Client* and establishes a session to the Agency A *Retrieval Manager* (RM) using CIP and sends the query to the Agency A RM
7. ≠ The RM then sends the query to the remote *Retrieval Managers* which pose queries to local collections and return results to the local agency ICS Gateway.
8. ≠ The *ICS Gateway* translates the returned result set into local format and returns the result set to the Client.
9. ≠ The human user evaluates the results and requests browse attributes for four data products of interest in ESA collections
10. Steps 3-8 repeated
11. The user decides to order the four products

Order Sub-Scenario

12. The local Client puts up an order specification form which the user fills out
13. The local Client sends an order quote request to the ICS Gateway
14. ≠ The *ICS Gateway* translates the order quote message into CIP format and the local product identifiers into appropriate CIP product identifiers
15. ≠ The *ICS Gateway* acts as a *CIP Client* and establishes a session to the Agency A *Retrieval Manager* (RM) using CIP and sends the quote request to the Agency A RM
16. ≠ The Agency A RM sets up an authenticated session with the ESA RM as Agency A via the CIP to obtain Agency A session options.
17. ≠ The Agency A RM sends the quote request to the ESA RM and requests a price estimate for the order.
18. ≠ The ESA RM forwards the quote request to the local Order Handling System (OHS) which returns the estimate to the ESA RM.
19. The ESA RM returns the quote to Agency A RM.
20. The Agency A RM forwards the estimate to the ICS Gateway
21. ≠ The *ICS Gateway* translates the returned message into local format and returns the message to the Client
22. The user reviews the estimate and requests the order be submitted

23. ≠ The *ICS Gateway* checks the user's credit via an interaction with the Agency A Billing and Credit Subsystem and on credit approval obtains an order number for local billing
24. ≠ The *ICS Gateway* translates the estimate approval format into CIP and forwards it to the Agency A RM which forwards it to the ESA RM which forwards it to the local OHS
25. ≠ The local OHS accepts the order and sends a status update of Order Acceptance to the ESA RM which forwards it to the Agency A RM which forwards it to the ICS Gateway
26. ≠ The *ICS Gateway* translates the message to the Agency A format and order number and informs the local Client and the local Billing and Credit subsystem of the order status
27. The human user logs off his local client and all sessions are terminated

8.2.1.3 Indirect Ordering Scenario

ICS Compatibility: Explanatory

General

The scope of this scenario is to show how a user places an order with a *Retrieval Manager* at which he is registered (*Retrieval Manager* - A) and, transparent to the user, the order is routed to another *Retrieval Manager* (*Retrieval Manager* - B) which has access to the products.

Assumptions

1. User has performed a search process and obtained the identifiers of a set of products which he wishes to order.
2. The user's agency and the data holding agency have an agreement that allows the user's agency to act as a proxy for its users to order data. The data holding agency will bill the user's agency for the data. The user's agency will bill the user for the data.
3. The order is placed with a *Retrieval Manager* (*Retrieval Manager* - A) with which the user is registered and has privileges sufficient to allow the order.
4. The Intermediary *Retrieval Manager* (*Retrieval Manager* - A) is authenticated with the *Retrieval Manager* which will fill the order (*Retrieval Manager* - B).
5. The order will be delivered in media, e.g. CD-ROM.
6. The user has established an authenticated session with *Retrieval Manager* - A.
7. *Retrieval Manager* - A has established and authenticated session with *Retrieval Manager*- B.

Expected Outputs

The user reviews a quote for the order, submits the order, and receives the products some time later.

Step Sequence

1. The *CIP Client* displays an order form which the user fills out.
2. User chooses to be charged by his own agency (not the agency that holds the data).
3. The *CIP Client* sends the order request to *Retrieval Manager* - A as part of an authenticated session.
4. *Retrieval Manager* - A determines the user's privileges based upon the user's group membership for that session. The group privileges allow this order request.
5. *Retrieval Manager* - A identifies the site from which data is being ordered (*Retrieval Manager* - B) based on information in the product identifiers in the order.

6. *Retrieval Manager* - A sends the order request and a group designation to *Retrieval Manager* - B as part of an authenticated session. (Note that the group designation in this session is for the *Retrieval Manager* - A session and may differ from the group of the client's session.)
7. *Retrieval Manager* - B determines the privileges based upon group membership. The group privileges allow this order.
8. *Retrieval Manager* - B forwards the order to the *OHS Translator* which converts the order into a local OHS order. The translator then passes the order to the OHS.
9. The OHS produces a quote and cost breakdown and assigns a quote number.
10. OHS sends quote, cost breakdown and quote number to *Retrieval Manager* - B (via the *OHS Translator*) which forwards it to *Retrieval Manager* - A which forwards it to the *CIP Client*.

[Steps 2-10 can be repeated by the user by changing and re-submitting the order specification to get data pricing information.]

11. The user reviews the quote and decides to submit the order. The *CIP Client* sends the order submittal to *Retrieval Manager* - A.
12. The group privileges for the user's session allow this order but determines that the order must be non-repudiatable. *Retrieval Manager* - A sends a non-repudiation request to the CIP Client
13. The *CIP Client* requests the user to confirm the order submittal, which the user does.
14. The *CIP Client* sends the order as a non-repudiatable message to *Retrieval Manager* - A.
15. *Retrieval Manager* - A sends order submittal to *Retrieval Manager* - B.
16. *Retrieval Manager* - B determines the group privileges associated with the session with *Retrieval Manager* - A and allows the order submittal.
17. *Retrieval Manager* - B passes the order submittal to the local *OHS* (via the *OHS Translator*).
18. OHS accepts the order, determines an expected order completion date, and returns an order submittal response to *Retrieval Manager* - B.
19. *Retrieval Manager* - B passes the order submittal response to *Retrieval Manager* - A.
20. *Retrieval Manager* - A notifies the local *OHS* (via the *OHS Translator*) that the order submittal has been accepted.
21. The OHS associated with *Retrieval Manager*-A does the accounting and billing associated with the order and the user's account.
22. *Retrieval Manager* - A passes the order submittal response to the CIP Client.
23. Possibly after the users session is closed, the OHS associated with *Retrieval Manager* - B fills the order and sends the bill to the OHS associated with *Retrieval Manager* - A.

8.2.1.4 Guide Search Scenario - WWW Search Engine

ICS Compatibility: Explanatory

General

A user will be able to discover ICS Guide documents through general Web search engines, such as Alta Vista, Yahoo, or Lycos,

Assumptions

In order for users of general Web search engines to find ICS guides the following must take place prior to the search:

- An ICS *Guide System* must be set up at least at one site.
- Guide documents must have been ingested into the system.
- The companies hosting Web search engines should be notified of the URL of one instance of the Sites Listing file icsdoc.html. Recall that this file will be mirrored at every ICS site.
- The Web search engine must have indexed the ICS guide documents, which it finds from icsdoc.html.

Expected Outputs

The user is presented with URL links to guide documents accessible in ICS which match the user's query.

Step Sequence

1. User submits a free-text search query to a general Web search site (such as Alta Vista). If they just enter strings that they expect will be in the ICS guides, they will find them. However, since these general Web search sites index all documents on the WWW, users will likely get matches of documents outside of ICS. They could narrow their search using known Guide Attribute/Keyword pairs. For instance: "AuthorName=John Doe".
2. The search engine looks up the URLs for the associated query strings in its index and displays the links for guide documents that contained the free-text. Note that while the user can use Guide Attribute/Keyword pairs because of the insertion of Meta tags, the search is still a free∞ text search. These search engines only use free-text.
3. The search engine responds back to the WWW Browser with a list of links.

8.2.1.5 Guide Search Scenario - ICS Client

ICS Compatibility: Explanatory

General

An ICS fielded guide search allows the user of an ICS Client to specify values for guide attributes, which will be in the list of guides returned. The IGP Client sends the FieldSearchForm IGP message to the ICS Guide Server.

Assumptions

- The user has a URL for an *ICS Guide Server*.

Expected Outputs

The user is presented with URL links to guide documents accessible in ICS which match the user's query.

Step Sequence

1. *ICS Client* connects to an ICS Guide Server using a *FieldSearchForm* message
2. The *ICS Guide Server* invokes the *icssearch* CGI script with the argument "searchform"
3. *icssearch* reads the Attributes Default File, generates a fielded search form HTML page, and sends it to the *ICS Client* to display. The form contains Guide Attribute names for labels for text boxes that the user can fill in. There is an additional text box with the label "Free Text" which the user can use to enter free-text to search. The form will have a submit button on it.
4. The user fills in the search form with desired entries
5. The ICS Client connects to the *Guide Server* and sends a *SearchFields* message.
6. The server responds to the SearchFields message by invoking *icssearch*, the ICS search engine, with the parameter value list.
7. The query return a list of guide URLs.
8. *icssearch* constructs an HTML page containing the list of guide URLs and passes it back to the *ICS Client*
9. The *ICS Client* displays the page of matching guide URLs to the user.

8.2.1.6 Guide Retrieval Scenario

ICS Compatibility: Explanatory

General

This scenario describes how a virtual guide document is created when requested by a client. The guide itself if pulled from the *Guide Document Archive* and additional information is added. The additional information includes metatags and URLs for related collections.

Assumptions

- The user has a URL for a guide document which is accessible through ICS. This URL may have been obtained from a previous search.

Expected Outputs

The guide document is displayed to the user in their stand-alone WWW browser or ICS Client.

Step Sequence

1. User initiates an HTTP connection using the URL for a browse document
2. Client connects to the ICS Guide Server at the site indicated in the URL, with the *GetVirtualDocument* IGP message.
3. Guide Server invokes *icsdoc* in the Guide Translator with path information of the guide document.
4. *icsdoc* looks up the guide in the Guide Metadata Database, retrieves the metadata for that guide, and constructs Meta tags
5. *icsdoc* reads the guide document from the *Guide Document Archive* using the path information supplied in the message.
6. *icsdoc* inserts the Meta tags into the header section of the guide

7. *icsdoc* looks up the guide in the Collections Mapping File, extracting the collection IDs for the guide. *icsdoc* constructs links to the data collections. The format of the collection link will depend on the type of client requesting the document, WWW Browser vs. ICS Client.
8. the Guide Server responds back to the Client with the guide document.

8.2.2 Collection Population Scenarios

This section contains scenarios concerning establishment of collections.

- Establishing collections in a Retrieval Manager for the first time
- Creating a new Provider Theme collection in response to a Earth Science Event

8.2.2.1 Making a CIP Compatible Catalogue Available

ICS Compatibility: Explanatory

General

A provider who works for a large company wants to make his scanned aerial pictures accessible through the ICS.

This scenario is roughly based on CEO-ES Scenario 4: Making a CIP compliant catalogue available.

Assumptions

The following assumptions apply to this scenario:

- The provider has an Internet connection and a UNIX workstation.
- The provider has an existing inventory system on a relational database system which catalogues all the data products archived at the company.
- The catalogue the provider wants to make available is an EO-data catalogue.

Expected Outputs

The catalogue of the provider becomes accessible for the ES users.

Step Sequence

1. The potential data provider attends a CEOS meeting and decides to host a *Retrieval Manager*
2. Reviews CEOS documentation describing ICS
3. Accesses the CEOS *Retrieval Manager* software distribution site
4. Retrieves RM source code
5. Configures the *Retrieval Manager* for his specific environment
6. Develops translator for local inventory searches reusing a skeleton *Catalogue Translator*.

7. ≠ Develops a gateway from the RM to his local Order Handling System (OHS) by reusing the local OHS provided with the RM
8. ≠ Establishes Provider Archive Collections for each of his existing datasets by developing Collection Descriptors for each of the datasets and an Explain database which lists the available services at his RM, and describes some product specific attributes which are used in the local catalogue systems to describe specific details of the individual photographs
9. ≠ Establishes a Provider Theme Collection which combines several existing datasets which contain aerial photographs and modifies the Explain Database to list the new Provider Theme Collection as a Key Access node
10. Establishes a root collection that references all the collections at the local site
11. ≠ Contacts the Global Collection Administrator via email and describes the datasets that have been established. The Global Collection Administrator advises the provider as to the keyword that should be used to characterize his collections and some remote collections that have similar themes
12. ≠ The provider modifies his root collection and his Provider collection to reflect the discussions with the Global Collection Administrator
13. Conducts local test of *Retrieval Manager* and collections
14. ≠ Send a message to the Global Collection Administrator announcing his desire to bring up a *Retrieval Manager* and join the ICS and puts the RM on-line to allow remote testing
15. ≠ The Global Collection Administrator performs integration testing on the new provider site, and when he is satisfied at the results, adds the root collection of the new provider site to the global collection and announces the availability of the new provider site and collections to the ICS community via email and the WWW.
16. ≠ The *ISA* at the new site continues to evolve his collections by adding new Provider Theme Archives and adding references to remote collections of interest to each of his collections

8.2.2.2 Collection Established for an Event

ICS Compatibility: Explanatory

General

This scenario demonstrates how a Provider Theme Collection is created. The scenario shows the interaction of the *ISA* and a scientist for the creation of the collection. The collection is created based on an event of particular weather patterns over the Andes.

This scenario is based on a scenario titled 'Climate, Erosion, and Tectonics in the Andes and other Mountain Systems,' which is ECS Scenario 22B, in [R22].

Assumptions

The following assumptions apply to this scenario:

- The user is a scientist at an agency which hosts a RM
- The user has discovered an interesting event analyzing data from an instrument.

Expected Outputs

The user wants to establish a collection for the event which his colleagues may access.

Step Sequence

1. A severe storm in the Andes is detected by user's review of MODIS Level 2 Imagery Products
2. ≠ User searches in ICS for other data products which overlap the event in temporal and spatial location.
3. ≠ The user establishes a hot collection based on the result set returned from his query. this results set contains data granules from MODIS, MISR, ASTER, GLAS, LANDSAT-7, ERS-2, ADEOS, and RADARSAT.
4. ≠ The user conducts incremental queries on the hot collection holdings to narrow the collection by determining the quality of each product and the degree of overlap with the storm track
5. ≠ The user establishes the final refined result set as a hot collection and deletes the earlier established hot collection
6. ≠ The user orders all the products remaining in his hot collection and applies various analysis techniques to detect the presence of the event in the other sensor data
7. ≠ The user uses hot collection editing tools to eliminate the products that do not show effects(e.g. landslides or floods) from the storm and contacts his local site *ISA* to request his hot collection be upgraded to a User Theme Collection.
8. ≠ The user writes a paper on the event and lists the URL for the collection requesting reviews by his colleagues to verify and augment his conclusions
9. ≠ The user receives several favorable reviews of his research and contacts his local *ISA* about the possibility of having the agency publicize and maintain the collection for long term preservation
10. ≠ The *ISA* and the agency science review board reviews the collection and the colleague comments and agrees to ingest the collection into the agency archive.
11. ≠ The *ISA* sends a form to the user requesting needed metadata about the collection. The user fills out the form and returns it to the *ISA*.
12. ≠ The *ISA* converts the user theme collection to a provider theme collection by upgrading the metadata, including the collection descriptor in the RM root collection.
13. The *ISA* advertises the collection via Email , bulletin boards and the CEO advertising service.
14. ≠ All ICS users are now able to access and search Andes Severe Weather Event Provider Theme Collection.

8.2.3 System Management Scenarios

ICS Compatibility: Explanatory

This section will contain scenarios concerning ICS System Management. As System Management is an ICS Release C focus, these section contains short descriptions which may be developed for Release C.

Retrieval Manager Registration. The scope of this scenario is to show how a *Retrieval Manager* becomes registered as an ICS *Retrieval Manager* and subsequently supports authenticated *CIP sessions* to allow ordering.

Planning a Retrieval Manager Outage. The scope of this scenario is to show how the *ISA*s work as a distributed management team. It is assumed that *ISA*s are trained in ICS Systems Administration procedures, a certain *Retrieval Manager* has been operational for some time and is remotely linked by many other *Retrieval Managers*, and the *Retrieval Manager* must be down from operations for several hours to change a piece of hardware. The expected output is that disruptions to ICS users are minimal and any users calls to *ISAs* are handled in an informed manner.

Response to Retrieval Manager Fault Condition. The scope of this scenario is to demonstrate the use of the *Retrieval Manager* monitoring functions by an operator in abnormal situations. It should be noted that the problems encountered in this scenarios are not representative of the ICS normal behavior and are presented here for illustration purposes. This scenario is based on CEO-ES Scenario 8: Middleware node operator - Use of the monitoring server.

8.3 Internal Interface Identification

Interfaces for the various ICS components have been stated in the multiple architectural views provided in the previous sections of the SDD. This section provides a summary of the interfaces between ICS components insuring consistency and completeness.

8.3.1 Retrieval Manager Interfaces

ICS Compatibility: MAA

The *Retrieval Manager* has the interfaces indicated in Table 8-3.

Table 8-3. Retrieval Manager Interfaces

Other ICS or Related Element	Interface	SDD Section
ICS Client	CIP sessions	3.5.1
ICS Client	Data Exchange	4.6
ICS Client	TCP/IP via National Internet	5.2.1
ICS Client	TCP/IP via World-wide Internet	5.2.1
Other z39.50 Clients	Z39.50, Version 2 or 3, sessions	3.5.1
Other z39.50 Clients	Data Exchange	4.6
Other *Retrieval Managers*	CIP sessions	3.5.1
Other *Retrieval Managers*	Data Exchange	4.6
Other *Retrieval Managers*	TCP/IP via National Internet	5.2.1
Other *Retrieval Managers*	TCP/IP via World-wide Internet	5.2.1
Other *Retrieval Managers*	TCP/IP via CEOSnet	5.2.1
Other *Retrieval Managers*	Secure Indirect Orders	6.2.4.4
Catalogue Translator	CIP sessions	3.5.1
Catalogue Translator	Data Exchange	4.6
OHS Translator	CIP sessions	3.5.1
OHS Translator	Data Exchange	4.6
UPS Translator	UPS Session	3.5.1
UPS Translator	Data Exchange	4.6
UPS Translator	Username/Passwords	6.2.4.3
ISA	Operator Interface	3.5.1
ISA	Operator Interface Data	4.6
ISA	Username/Passwords	6.2.4.3
Collection Management Tool	Collection Data Base Modification	3.5.1
Collection Management Tool	Data Exchange	4.6
Monitoring and Control Tool	*Retrieval Manager* Management	3.5.1
Monitoring and Control Tool	Data Exchange	4.6
ICS Gateway	CIP Sessions	3.5.1
All CIP Interfaces	Use of TCP/IP	5.1.1
All CIP Interfaces	CIP to TCP Mapping	5.1.3.1
Distributed CIP Interfaces	Session Management	5.1.4
DNS	Directory Service	5.1.6
Site Physical Facilities	Physical Security Control	6.2.3
Test Equipment	Functional Tests	7.2

8.3.2 ICS Client Interfaces

ICS Compatibility: MAA

The *ICS Client* has the functional interfaces indicated in Table 8-4.

Table 8-4. ICS Client Application Interfaces

Other ICS or Related Element	Interface	SDD Section
Retrieval Manager	CIP sessions	3.5.2
Retrieval Manager	TCP/IP via National Internet	5.2.1
Retrieval Manager	TCP/IP via World-wide Internet	5.2.1
Retrieval Manager	Data Exchange	4.6
HTTP/CIP Gateway	CIP sessions	3.5.2
Human user	Data to user	3.5.2
Guide Server	HTTP Connection	3.5.2
All CIP Interfaces	Use of TCP/IP	5.1.1
All CIP Interfaces	CIP to TCP Mapping	5.1.3.1
All IGP Interfaces	Use of TCP/IP	5.1.1
All IGP Interfaces	HTTP use of TCP	5.1.5
DNS	Directory Services	5.1.6

8.3.3 ICS Site Administrator (ISA) Interfaces

ICS Compatibility: MAA

The *ISA* has the operational interfaces indicated in Table 8-5.

Table 8-5. ICS Site Administrator Interfaces

Other ICS or Related Element	Interface	SDD Section
Retrieval Manager	Operator Interface	3.5.8
Retrieval Manager	Physical Security	6.2.3
Retrieval Manager	Operator Interface Data	4.6
Collection Management Tool	Operator Interface	3.5.8
Monitoring and Control Tool	Operator Interface	3.5.8
ICS User	Username/Password	6.2.4.2
Other *ISAs*	Inter-Agency Billing Agreements	6.2.4.3
Other *ISAs*	Inter-Agency Security Agreements	6.2.4.3
Other *ISAs*	Group Management	6.2.4.4
Other *ISAs*	Administrative Security Controls	6.2.2
Other *ISAs*	System Administration	7.
Interfaces outside of ICS	OHS, UPS, Catalogue, Archive, Guide Document Archive.	3.5.8
OHS Translator	Maintain and Operate	3.5.8
UPS Translator	Maintain and Operate	3.5.8
Catalogue Translator	Maintain and Operate	3.5.8
Guide Indexer	Maintain and Operate	3.5.8
ICS Federation Management	System Management Operations	7

8.3.4 Collection Management Tool (CMT) Interfaces

ICS Compatibility: MAA

The CMT has the interfaces indicated in Table 8-6.

Table 8-6. Collection Management Tool Interfaces

Other ICS or Related Element	Interface	SDD Section
Retrieval Manager	Collection Data Base Modification	3.5.9
Retrieval Manager	Data Exchange	4.6
ISA	Operator Interface	3.5.9
Guide Server	Update Guide Collection Mapping File	3.5.9
Interfaces outside of ICS	Data file ingest	3.5.9

8.3.5 Monitoring and Control Tool (MCT) Interfaces

ICS Compatibility: MAA

The MCT has the interfaces indicated in Table 8-7.

Table 8-7. Monitoring and Control Tool Interfaces

Other ICS or Related Element	Interface	SDD Section
Retrieval Manager	*Retrieval Manager* Management	3.5.10
Retrieval Manager	Data Exchange	4.6
ISA	Operator Interface	3.5.10
Guide Server	Monitor Status and send commands	3.5.10
Guide Indexer	Monitor Status and send commands	3.5.10
Guide Translator	Monitor Status and send commands	3.5.10
OHS Translator	Monitor Status and send commands	3.5.10
UPS Translator	Monitor Status and send commands	3.5.10
Catalogue Translator	Monitor Status and send commands	3.5.10
Interfaces outside of ICS	SSM	3.5.10

8.3.6 Guide Server Interfaces

ICS Compatibility: MAA

The Guide Server has the interfaces indicated in Table 8-8.

Table 8-8. Guide Server Interfaces

Other ICS or Related Element	Interface	SDD Section
ICS Client	IGP Connection	3.5.11
ICS Client	Data Exchange	4.7.1
Guide Indexer	IGP Connection	3.5.11
Guide Translator	IGP Connection	3.5.11
Other *Guide Indexers*	IGP Connection	3.5.11
CMT	Update Collection Mapping File	3.5.11
Interfaces outside of ICS	SSM	3.5.11
All IGP Interfaces	Use of TCP/IP	5.1.1
All IGP Interfaces	HTTP use of TCP	5.1.5
DNS	Directory Services	5.1.6
CEOSnet	Network Connectivity	5.2.1

8.3.7 Guide Indexer Interfaces

ICS Compatibility: MAA

The Guide Indexer has the interfaces indicated in Table 8-9.

Table 8-9. Guide Indexer Interfaces

Other ICS or Related Element	Interface	SDD Section
Guide Server	Update Guide Metadata Database	3.5.12
Guide Server	Data Exchange	4.7.1
Other *Guide Servers*	Update Guide Metadata Database	3.5.12
Other *Guide Indexers*	Notification of new URL	3.5.12
Interfaces outside of ICS	SSM	3.5.12
All IGP Interfaces	Use of TCP/IP	5.1.1
All IGP Interfaces	HTTP use of TCP	5.1.5
DNS	Directory Services	5.1.6
CEOSnet	Network Connectivity	5.2.1

9. ICS MINIMUM SITE CONFIGURATION

9.1 ICS Minimum Site Compatibility

ICS Compatibility: Mandatory

This section defines the required minimum configuration for a site which wishes to be considered ICS compatible. The minimum site is based on the CEOS policy which anticipates that members will provide the following: collection, product, and explain searches.

To be ICS compatible, a site must at least meet the following:

- Comply with the design in the SDD paragraphs with mandatory ICS Compatibility.
- Provide the elements listed in Section 9.2
- Support the CIP messages listed in Section 9.3
- Provide data listed in Section 9.5
- Support the operations listed in Section 9.6

Note that this section does not define CIP Compatibility, which is defined in the CIP Specification [R3]. The relationship between CIP and ICS compatibility is addressed in Sections 1.1 and 2.1.3 of the SDD.

9.2 ICS Elements for a Minimum Site

ICS Compatibility: Mandatory

For ICS compatibility, a site must provide the ICS elements listed in Table 9-1.

Table 9-1. ICS Elements for a Minimum Site

Element Name
Retrieval Manager
ISA

9.3 CIP Messages for a Minimum Site

ICS Compatibility: Mandatory

For ICS compatibility, a site's Retrieval Manager must support the CIP messages listed in Table 9-2.

Table 9-2. CIP Messages for a Minimum Site

CIP Message Name
initializeRequest
initializeResponse
searchRequest
searchResponse
presentRequest
presentResponse
segmentRequest
deleteResultSetRequest
deleteResultSetResponse
resourceControlRequest
resourceControlResponse
triggerResourceControlRequest
resourceReportRequest
resourceReportResponse
close

9.4 IGP Messages for a Minimum Site

ICS Compatibility: Explanatory

As support of Guide is not required at a minimum site, no IGP messages are required.

9.5 ICS Data for a Minimum Site

ICS Compatibility: Mandatory

For ICS compatibility, a site must provide the data listed in Table 9-3.

Table 9-3. ICS Data by for a Minimum Site

Element Name
CDB
Explain Database
Session Management Data
Use of ICS Valids

9.6 ICS Operations for a Minimum Site

ICS Compatibility: Mandatory

For ICS compatibility, a site must support the operations listed in Table 9-4.

Table 9-4. ICS Operations for a Minimum Site

Operational Activity
Retrieval Manager nominal operations: 24 hours per day, 7 days per week.
Trained *ISA* Staff: operations staff at the site trained as ICS Site Administrators.
ISA Response Time: maximum time of 4 hours for ISA at a site to begin responding to an ICS Event
Perform Collection Maintenance as defined in ICS Collection Manual